The Impact of Consumer Privacy Behavior on the Purchase Decision Process of Smart Home Internet of Things (IoT) Devices

Mercy Ebenezer

A thesis

submitted in partial fulfillment of the

requirements for the degree of

Master of Science in Computer Science & Software Engineering

University of Washington

2017

Committee:

Marc Dupuis

William Erdly

Yang Peng

Program Authorized to Offer Degree:

Computing and Software Systems

University of Washington

Abstract

The Impact of Consumer Privacy Behavior on the Purchase Decision Process of Smart Home Internet of Things (IoT) Devices

Mercy Ebenezer

Chair of the Supervisory Committee:
Dr. Marc Dupuis
Computing and Software Systems

Privacy issues in smart home Internet of Things (IoT) devices remain unresolved despite its fast growth in the technological and business front. Notwithstanding federal institutions' initiatives to increase consumer awareness and business accountability towards privacy violations, there is a dearth of corrective measures that fix the privacy issues in smart home IoT devices. The lack of simple privacy protection measures in smart home IoT devices is the primary reason for consumers to overlook the institutions' privacy awareness initiatives. As a result, privacy is traded off for *convenience* and this reflects in the choices consumers make during their purchase decision process.

In this exploratory study, I have performed in-depth analysis of consumer behavior towards adopting privacy protection measures for smart home IoT devices during the purchase decision process. Three privacy protection measures have been stated and a consumer's attitude towards

these three measures is evaluated. Qualitative research methods are a useful instrument in this evaluation.

First, content analysis on customer reviews was performed to understand the main factors that influence a purchase decision process. The customer reviews were collected from Amazon's best sellers in the "smart home" category for the top 10 smart home IoT devices.

Second, qualitative data analysis of interviews with study participants provided extensive insight into possible factors that affect a consumer's privacy protection behavior during the purchase decision process. Lack of time, effort, and resources to adopt privacy behavior were the factors observed during the data analysis process.

In conclusion, the study informs on the significance and impact of privacy behavior on the purchase decision process and proposes disruptive innovation to attain sustainable business growth in smart home IoT devices.

Table of Contents

List of tables

List of figures

Dedication

This work is dedicated to my parents, Ebenezer and Hannah; my sister, Rebekah Edwin; my brother-in-law, Anand Edwin; and my niece and nephew, Joanna Edwin and Elijah Edwin.

Acknowledgments

This thesis study has been one of the most enriching experiences of my academic life. It has helped me explore an expanse of knowledge in the field of human computer interaction with information systems, and the impact of HCI on the business of the Internet of Things (IoT) systems.

First, I would like to acknowledge my chair, Dr. Marc Dupuis, for his constant guidance throughout the journey. His patience and constructive feedback have helped me bring the thesis work to completion.

I would like to acknowledge my committee members, Dr. William Erdly and Dr. Yang Peng. I am grateful to Dr. William Erdly for helping me with the "Research Methods" course and providing necessary feedback during the initial phases of the research work.

I would like to acknowledge my parents, Ebenezer and Hannah; their love, support, and sacrifice continuously motivated me to bring the thesis work to completion.

Finally, I would like to acknowledge my sister and her family for their love and enduring care.

Chapter 1: Introduction

Background to the Research

The Internet of Things (IoT) connects device with device, people with people, and people with device. This connection is made possible through several technologies and communication solutions that function to perform a wide range of tasks (Atzori, Iera, & Morabito, 2010). A more structured definition of IoT given by the U.S. National Intelligence Council is as follows (McGrath & Scanaill, 2013, p. 99):

> The "Internet of Things" is the general idea of things, especially everyday objects, that are readable, recognizable, locatable, addressable, and controllable via the Internet - whether via RFID, wireless LAN, wide-area network, or other means.

IoT has a wide range of application areas: transportation and logistics, healthcare, smart environment (home, office, plant), and personal and social domains (Atzori et al., 2010). These domain areas connect different parts of the community and enable each entity within that community to work efficiently. For instance, a home IoT device that regulates the home temperature also sends sensor data to the electricity company to optimize the electricity usage appropriately for its consumer (Gubbi, Buyya, Marusic, & Palaniswami, 2013). This large-scale expansion and integration is associated with an increase on the business front as well. According to Business Insider, $6 trillion will be spent on IoT solutions in the next 10 years and 34 billion devices will be connected to the Internet by 2020, more than triple the 10 billion connected devices in 2015 (Camhi & Greenough, 2016).

Besides the application areas mentioned above, the need for smart home automation systems is increasing at a good pace (The Deloitte Consumer Review, 2016). It is estimated that smart home IoT devices will exhibit the highest increase in the next five years when compared to other subcategories of smart city devices, such as health care, public services, smart commercial buildings, transport, and utilities ("Gartner Says Smart Cities Will Use 1.6 Billion Connected Things in 2016," 2015). This finding from Gartner and The Deloitte Consumer Review highlights the importance of considering smart home IoT devices and the surrounding privacy issues and concerns.

Smart home IoT devices are built with many sensors (cameras, microphones, motion detectors) and actuators (light, speakers, locks) (Notra, Siddiqi, Gharakheili, Sivaraman, & Boreli, 2014). Their large infrastructure has multiple points of data entry and exit. The large number of devices connected within the infrastructure is extensive, and therefore it is difficult to establish an integrated system to monitor these multiple points of entry and exit. The sensors form a significant part of the infrastructure and collect a large amount of data (Gubbi et al., 2013). This data is then transferred to multiple other devices and applications within the infrastructure. The smart home IoT architecture is illustrated in Figure 1.

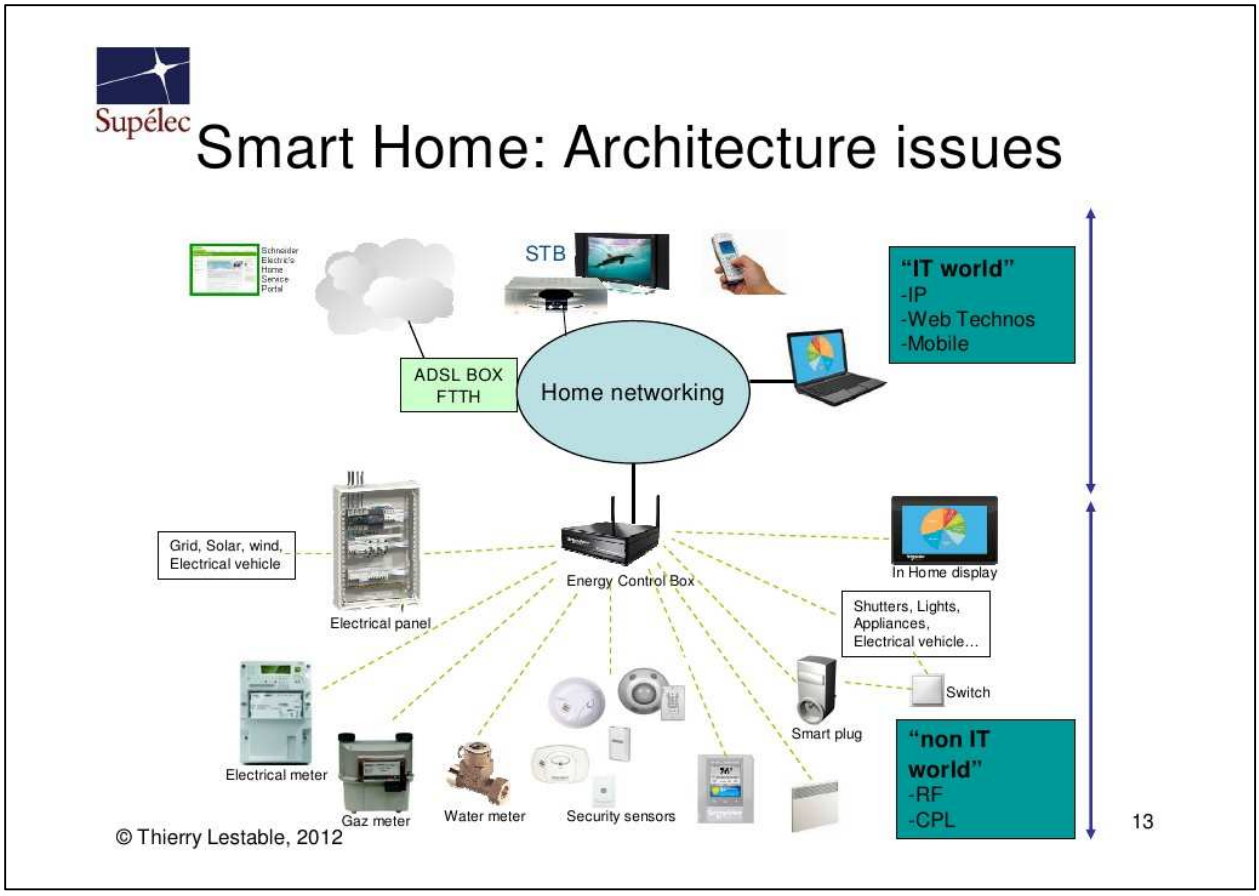

Figure 1: Interconnection of smart home IoT devices (Lestable, 2012)

Besides this complexity in the infrastructure of the smart home IoT devices, the combination of data streams that run throughout it is convoluted. In addition, the creative interconnection of everyday objects and devices within the infrastructure can be dangerous because of the large amount of sensitive data collected, shared, and stored. This poses a threat to consumer privacy (In, 2017). For instance, the video streaming feature of a home monitoring system transfers a recorded video data file to a mobile application or a cloud storage unit. Then, the built-in notification feature of the system effectively notifies the community's security authority in the case of a burglary. Although this kind of reporting is beneficial to the consumer,

the large-scale system integration with the different entities of the community allows consumers to be easily identified, especially when metadata such as timestamps and geo locations are present along with the original video data stream (In, 2017). This type of surveillance, lack of anonymity, and de-identification of consumer data raises privacy concerns.

Privacy issues in smart home IoT devices are a major social concern because of the inappropriate methods of data collection, sharing, and storing (Gubbi et al., 2013; Zorzi, Gluhak, Lange, & Bassi, 2010). The existence of these privacy issues is attributed to the large infrastructure that governs the IoT ecosystem (In, 2017). Privacy issues are derived from different privacy categories: Identity, Location, Search Query, and Digital Footprint (In, 2017). One of the manifestations of the identity privacy issue is constant monitoring of consumers without their knowledge. This is commonly known as the "big brother like control" (Zorzi et al., 2010). This type of invasion into a consumer's personal space often leads to privacy violations and raises definitive privacy concerns (In, 2017, p. 201).

Privacy and security issues are interlinked in smart home IoT devices (Sivaraman, Gharakheili, Vishwanath, Boreli, & Mehani, 2015). These devices collect a large volume of sensitive data, such as personally identifiable information (PII) and video and audio data files, as well as non-sensitive data. There is a high possibility for consumers to be victimized by cyberattacks on IoT systems because of easy access to sensitive data available on the Internet (Perera, Ranjan, Wang, Khan, & Zomaya, 2015). As a result, these systems have been under great scrutiny. The poor security features in home IoT devices do not ensure secure data collection, storing, and sharing—and consequently consumers' data is at risk (Sivaraman et al., 2015).

Several federal institutions have raised concerns over the inappropriate data collection methods employed by IoT solution providers. Workshops, seminars, and press releases are some of the prevalent initiatives to address privacy issues in IoT systems (Ohlhausen, 2014). The solution providers of smart home IoT devices must begin to consider privacy issues with greater seriousness to best serve consumers' interests and needs (Ohlhausen, 2014). Possible ways for this to occur include fulfilling privacy requirements, such as data privacy, anonymity, pseudonymity, and unlinkability (In, 2017). However, IoT solution providers' responses to these initiatives are less pronounced when compared to their rampant efforts to expand their business or to exhibit significant progress in the technological front (Camhi & Greenough, 2016; The Deloitte Consumer Review, 2016).

When IoT solution providers exhibit little or no interest in fulfilling privacy requirements, the responsibility of privacy protection shifts to consumers. However, consumers fall short of adopting privacy protection measures.

Therefore, this study explores the possibility of adopting consumer privacy behavior as it relates to the privacy protection measures during the purchase decision process of smart home IoT devices. Three privacy protection measures are relevant to this study: establishing privacy preferences, adopting privacy education, and using a privacy testing tool. Consumer purchase decisions on smart home IoT devices are a good reflection of a consumer's ability to ascertain and adopt privacy protection measures during their purchase decision process.

There lies a great ambiguity, however, in understanding whether the abovementioned privacy protection measures are well known and easily accessible. It is also important to find out if these measures help consumers to completely overcome their privacy concerns as it relates to the purchase of a particular device. A comparative analysis that theoretically discusses easy

accessibility and the importance of privacy protection measures during the purchase decision process is presented in this study.

The information security behavior towards free information services (social media platforms, mobile applications, search websites) or electronic devices of daily use (phones, laptops, personal computers, tablets, etc.) (Katell, Mishra, & Scaff, 2016) is easy to adopt because the resources for it are easily accessible. For instance, free information services like Facebook provide multiple ways for users to hide their private or sensitive data to prevent others from viewing it. Similarly, laptops or PCs have built-in packages that constantly remind users to secure their devices and data through emails or forced system updates. The forced system updates often annoy users but they potentially accomplish updating the system with the necessary security patches. However, this is not the case for smart home IoT devices. Instead, privacy protection measures for these devices are difficult to find and hard to follow. One manifestation of this difficulty is recognized in the design of the home IoT device displays and the attached privacy policy statements.

Privacy policy statements for home IoT devices often appear on the official IoT device's website rather than the product package (Peppet, 2014). This is often inconvenient for consumers and does not account for best practices in privacy protection. The statements also are long and contain complicated language that makes them difficult for the user to comprehend and consequently exhibit protective behavior. In addition, home IoT devices have small displays and no clear indication of the input and output areas restrict the consumers from reading the policy statements on the device itself (Peppet, 2014).

For these reasons, this study focuses on understanding the implications of the abovementioned limitations as it relates to the adoption of consumer privacy behavior during the purchase decision process for smart home IoT devices.

Propositions, Research Issues, Research Problem, and Contributions

Privacy issues in smart home IoT devices are a major concern among many consumers and researchers. The impact of this concern on the purchase decision process is evaluated by analyzing a consumer's privacy behavior. The lack of fervor in exercising privacy protection behavior during the purchase decision process can be associated with factors such as self-efficacy, response efficacy, and response costs. These factors are derived from the popular behavioral theory, protection motivation theory (PMT). Besides self-efficacy, response efficacy, and response costs, PMT includes perceived threat severity and perceived threat vulnerability (Norman, Boer, & Seydel, 2005)

Several researchers have used PMT to understand and analyze information security behavior for a wide variety of applications and devices (Dupuis, 2014). Cognitive factors, such as threat appraisal and threat severity, have been studied in detail to understand its impact on the adoption of privacy behavior using privacy enhancement techniques (PET) (Matt et al., 2016).

Besides PMT, other behavioral theories, such as the theory of planned behavior (TPB) and the theory of reasoned action (TRA), have been instrumental in understanding the correlation between the human attitude and the behavioral intent as it relates to complying with security policies in information systems (Ifinedo, 2012). This study will employ PMT to explain the factors

that affect privacy behavior during the purchase decision process. A detailed reasoning on the use of PMT is provided in Chapter 2.

The general notion of consumer buying behavior in an online environment requires necessary consideration as it forms the baseline understanding for consumer privacy behavior during the online purchase decision process.

Consumer behavior while shopping online is well explained through theories such as the technology acceptance model (TAM), flow theory, and marketing theory (Koufaris, 2002). This collection of theories derives from information systems, marketing, and psychology (Koufaris, 2002). It primarily emphasizes the factors that enable consumers to effortlessly engage in purchasing decisions. These theories address aspects of human cognition, such as perceived risk and uncertainty, that have the potential to dissuade a consumer from purchasing a particular product (Koufaris, 2002; Murray, 1991).

With this understanding of consumer behavior during the purchase decision process in mind, it is also essential to consider consumer privacy behavior. Research in information systems supports the notion that consumers prefer to protect their privacy when privacy protection methods are simple (Berendt, Günther, & Spiekermann, 2005; Spiekermann, Grossklags, & Berendt, 2001). However, privacy behavior changes when the consumer enters the online shopping environment (Berendt et al., 2005).

The relationship between consumer privacy behavior during the purchase decision process and the interplay of constructs (self-efficacy, response efficacy, and response costs) requires in-depth investigation and this leads to the following research problem:

Research Question (RQ): What is the impact of consumer privacy behavior on the purchase decision process of smart home IoT devices?

Justification for the Research

Privacy issues in smart home IoT devices are increasing at an alarming rate (Sivaraman et al., 2015). The security features in these devices have improved with the use of Internet Protocol version 6 (IPv6), but continue to face challenges in protecting user data (Evans, 2011). Secure data aggregation is essential within the large IoT infrastructure and can be achieved only through effective security features (Gubbi et al., 2013).

IoT devices are vulnerable to cyberattacks, which results in data leakage over the Internet and possible identity threats. For this reason, private and sensitive data must be secured over the IoT infrastructure and the Internet. IoT businesses must be able to address privacy issues in home IoT devices and adopt corrective measures so that consumers' trust and confidence in the devices remains constant. By doing so, IoT solution providers will be able to fulfill the privacy requirements suggested by federal institutions such as the Federal Trade Commission (FTC) (Ohlhausen, 2014).

Despite the privacy issues, home IoT devices are convenient and beneficial for homeowners because they provide a wide range of services (Sivaraman et al., 2015). Besides home owners, these devices perform various functions within a community and provide convenience (In, 2017). Such functionalities continue to motivate consumers and communities to invest in these devices despite the privacy issues and concerns (Weinberg, Milne, Andonova, & Hajjat, 2015).

Methodology

Qualitative Research Methods

This study used qualitative data analysis procedures to understand the effect of self-efficacy, response efficacy, and response costs in adopting privacy protection measures during the purchase decision process.

First, 500 customer reviews were collected from Amazon's best sellers of the "smart home" category for the top 10 smart home IoT devices. The reviews were collected according to ratings and a variety of review groupings. The reviews were grouped in a factorial manner based on the rating scale and the review category. This data collection process was employed to understand the consumer privacy behavior during the purchase decision process.

After the data collection, appropriate qualitative data analysis procedures were used to code the large number of reviews. The coding strategies efficiently generated six major themes. These themes were later applied throughout the data to produce subthemes. Some necessary subthemes were introduced and removed accordingly to reconcile the differences within the large data set. After the coding process, the themes were explained and useful insights were recorded.

Second, interview sessions were conducted among 18 student participants from the University of Washington Bothell. Participants were selected to maximize a gender balance and diversity of educational backgrounds (i.e., majors). The participants were questioned on the following aspects: privacy behavior, knowledge of privacy issues in home IoT devices, impact of privacy behavior on the purchase decision process, and so on. The interview data was later transcribed and coded using appropriate coding strategies. The insights from the coding process

were noted. The relevant conclusions appear in chapter five and a detailed explanation of both methodologies appears in chapter three.

Definitions

This section provides a list of definitions of words and phrases used in this thesis to ensure a common understanding of them to help facilitate the discussion.

- **Smart home IoT device:** These devices automate regular home devices, such as home appliances, home lighting, air-conditioning, heating, surveillance cameras, and door locks. They do so with the help of cloud services, web applications, sensors, network technologies, and so on (Wan & Low, 2013). This report uses the terms "smart home IoT devices" and "home IoT devices" interchangeably.
- **Self-efficacy:** The belief of an individual to successfully perform an action (Norman et al., 2005; Woon, Tan, & Low, 2005).
- **Response cost:** The cost (money, effort, or time) associated with engaging in protective measures that assures mitigation of the perceived threat (Norman et al., 2005; Woon et al., 2005).
- **Verified purchases:** This category appears under one of the filter options in customer review section on the Amazon website. This option highlights a customer review written by a consumer who has bought the product.
- **Rating scale:** The rating scale is a gold star on e-commerce websites like Amazon.com that allow consumers to express how much they like (or dislike) the product. The scale ranges from 1 (negative rating) to 5 (positive rating), with 3 as the neutral rating.

- **Review group:** The review group represents two categories of customer reviews: top and recent. Top reviews are those voted as most helpful reviews by consumers buying the same product. And, the recent reviews are those characterized by the latest date on which the review was posted.
- **Top 10 smart home devices:** The top 10 home IoT devices were selected from the Amazon.com website from the best seller's category for smart home devices. This selection was performed on 02/14/2017.

Delimitations of Scope, Key Assumptions, and their Justifications

Study Participant Selection

The study participants were recruited from the university campus. This convenience sample was chosen keeping in mind that home IoT devices are common among most individuals.

IoT Category Selection

This study is restricted to understanding consumer privacy behavior for smart home IoT device consumers. The smart home IoT category was chosen after analyzing the importance of this category from the business profitability perspective ("Gartner Says Smart Cities Will Use 1.6 Billion Connected Things in 2016," 2015; The Deloitte Consumer Review, 2016). For this purpose, smart home IoT devices were selected and the customer reviews for these devices was collected.

Although many study participants did not own smart home IoT devices because they were not homeowners yet, they were aware of the popular home IoT devices such as Alexa, Nest, Philips Hue Light bulbs and so on.

Consumer Privacy Behavior

This study reviews three privacy protection measures: establishing privacy preferences, adopting privacy education, and using a privacy testing tool. Privacy preferences refer to the exclusivity displayed by consumers with respect to the disclosure of personal and sensitive information. Privacy education comprises reading, reviewing, and analyzing online resources such as blogs, forums, technical articles, and published reports that educate individuals on privacy issues or concerns in IoT systems. A privacy testing tool tests or scans an IoT device to generate a report on privacy violations and inappropriate data collection, storing, and sharing methods.

Purchase Decision Process

This is the process that consumers follow while buying a product. It begins with researching information on the product until the final purchase of the intended product. In this study, the purchase decision process is restricted to the online environment, specifically e-commerce websites like Amazon.com.

Selection Criteria for Top 10 Smart Home IoT Devices

The selection for the top 10 devices was performed on Amazon's best sellers in the smart home category on February 14th, 2017. Multiple iterations were followed to finalize the selection list because best seller tags on the devices tend to change according to sales at a given point in time. The list of top 10 smart home IoT devices appears in Appendix C.

Conclusion and Outline of the Report

Adopting privacy behavior can help address privacy issues and concerns in home IoT devices. This protective behavior is not very different from that of information security behavior

towards free online information services. The primary reason for neglecting privacy behavior is largely due to lack of resources providing privacy education to smart home IoT device consumers.

This study establishes privacy behavior by adopting three privacy protection measures: establishing privacy preferences, adopting privacy education, and using a privacy testing tool. These measures provide extensive knowledge to the consumer on existing privacy issues or concerns as they relate to the purchase of smart home IoT devices. However, a few factors have the potential to prevent consumers from adopting privacy behavior during their purchase decision process. These factors are studied with the help of the behavioral theory, protection motivation theory (PMT). Three of the constructs of PMT are self-efficacy, response efficacy, and response cost, which assist in explaining consumer privacy behavior during the purchase decision process.

The remainder of the thesis is as follows. Chapter 2 provides extensive information on research issues through a literature review of past work and a research model. It emphasizes the importance of privacy behavior and its impact on the purchase decision process. The research model is instrumental in explaining the implication of the PMT's constructs as it relates to the consumer privacy behavior and the purchase decision process.

Chapter 3 provides a detailed explanation on the methodologies used in this study. The chapter focuses on a discussion of the qualitative research methods used. It also contains comprehensive justifications for the employed research methods, explains the process of data collection, and elaborates on the research procedures instrumental to the data collection and data analysis phases.

Chapter 4 provides an analysis of the data obtained. The patterns of data from employing qualitative data analysis procedures on interview data and customer reviews are noted.

Chapter 5 discusses the implication of the results obtained from the data analysis process. It also discusses limitations of the study and recommendations for future research.

Chapter 2: Research Issues

Introduction

Protection Motivation Theory (PMT) forms the basis of this study and its constructs-self-efficacy, response efficacy, and response costs help us to understand the factors that affect a consumer's privacy behavior. Several studies of information systems use PMT to understand an individual's security behavior and ability (or inability) to exercise protective behavior in the event of risks, such as malware attacks on PCs or wireless home networks. Similarly, the adoption of protective behavior during the purchase decision process for home IoT devices is analyzed by understanding the general consumer buying behavior in an online environment.

Consumer buying behavior in the online environment is studied with respect to factors such as self-efficacy, response efficacy, and response costs. The similarities in consumer buying behavior and consumer privacy behavior are evaluated by reviewing the abovementioned factors. In addition, privacy protection measures with respect to free online information services are also reviewed to understand the privacy behavior of online users. This is later contrasted with the privacy behavior of home IoT device consumers during their purchase decision process.

The subsequent sections discuss PMT and its constructs self-efficacy, response efficacy, and response costs. The section on research problem theory provides insight into the development of consumer privacy behavior during the purchase decision process. Finally, the research model which guides the study, appears at the end of the chapter.

Parent Theories and Classification Models

This section discusses the different application areas that have used PMT to explain protective behavior in response to threat events. The two primary areas are human behavioral interaction with information systems and protective behavior towards health issues.

Several researchers have used PMT to understand the interaction of human behavior with information systems. The end user's likelihood of compliance with security policies in information systems is studied through the constructs of PMT (Herath & Rao, 2009). Organizational commitment and social influence also affect a user's compliance intention.

In one study, PMT was employed to study information security behavior of home users (Dupuis, 2014). Specifically, constructs such as perceived threat severity, perceived threat vulnerability, perceived response efficacy, self-efficacy, and perceived costs were analyzed with respect to trait affect. Similarly, PMT has been useful in understanding an employee's attitude towards complying with the organization's security policies (Bulgurcu, Cavusoglu, & Benbasat, 2010). In this study, an employee's compliance behavior was evaluated with respect to threat appraisal and coping appraisal. That is, an employee engages in protective behavior after examining the risk involved in non-compliance with the organization's security policies (Bulgurcu et al., 2010).

Furthermore, PMT has been used in several other disciplines, such as healthcare, where the coping mechanisms relate to health threats (Dupuis, 2014; Rippetoe & Rogers, 1987). The theory has been an integral part of several studies in the field of information systems. A list of research studies that emphasize protective behavior using PMT is provided in Table 1.

Table 1: Research studies that emphasize protective behavior using PMT

Primary Subject	Author(s) and Year
Impact of cognitive factor and personality traits on privacy protective behavior	(Matt et al., 2016)
Recommended behavior towards securing home wireless network	(Woon et al., 2005)
Employee behavior towards compliance to security policies	(Vance, Siponen, & Pahnila, 2012)
Home security behavior	(Anderson & Agarwal, 2010)
Online privacy protection behavior of young adolescents	(Youn, 2009)
A threat control model for information security behavior	(Workman, Bommer, & Straub, 2008)

The following sections examine PMT in detail and explain the constructs—self-efficacy, response efficacy, and response costs—that are foundational to the current study.

Protection Motivation Theory

PMT has been used in past studies to understand an individual's coping mechanism in response to a risk (Norman et al., 2005). The theory was first introduced by Rogers in 1975 and included the constructs- perceived vulnerability, perceived severity, response efficacy, and response costs (Youn, 2009). These constructs are explained as follows.

Perceived vulnerability is the likelihood of the occurrence of a risk to an individual, while perceived severity is the perceived impact of the risk (Norman et al., 2005; Youn, 2009). The

individual's belief that the recommended behavior is able to mitigate the risk is known as response efficacy (Norman et al., 2005; Youn, 2009) and the cost associated with such a behavior is represented by response costs (Norman et al., 2005; Woon et al., 2005)

In 1983, Rogers extended PMT to include self-efficacy to explain cognitive factors that mediate behavior (Dupuis, 2014; Norman et al., 2005). Self-efficacy is an individual's belief in the ability to engage in a particular protective behavior. The overall structure of the PMT framework is discussed next.

The coping mechanisms in response to fear motivate an individual to exhibit protective behavior. This is explained by two processes: threat appraisal and coping appraisal (Woon et al., 2005). Threat appraisal consists of perceived threat severity and perceived threat vulnerability (Woon et al., 2005). Coping appraisal comprises self-efficacy, response costs, and response efficacy (Ifinedo, 2012).

Application of PMT

In this study, a fear appeal may be associated with privacy violations that arise from constant monitoring of consumers of home IoT devices and this leads to the "paranoid feeling". The home IoT devices with built-in IP traceable web cams have the potential to instill fear in its consumers. In general, these fear appeals are a result of inappropriate data collection, sharing, and storing of consumers' sensitive or private data. For instance, these devices collect audio and video data that could be leaked into the Internet through insecure mobile application interfaces and cloud-based web services (HP Inc., 2014).

To overcome these fear appeals, constructs from the coping appraisal process (self-efficacy, response efficacy, and response costs) are considered to understand the factors that prevent a consumer from adopting privacy behavior in the event of a threat.

Self-Efficacy

In this study, self-efficacy describes a consumer's belief in her ability to engage in specific protective behavior in response to a privacy concern while purchasing a home IoT device. Adopting privacy protection behavior enables a response to a privacy concern. This adoption is made possible through three privacy protection measures: establishing privacy preferences, adopting privacy education, and using a privacy testing tool. The self-efficacy levels are high when a consumer is confident in exercising her ability to react to a privacy concern and takes measures to protect her privacy.

Response Efficacy

According to PMT, response efficacy represents an individual's belief that the recommended protective behavior has the potential to successfully mitigate the threat. In this study, a consumer must believe that adopting privacy behavior will prevent her from identity theft or secure her sensitive data on the Internet. The consumer must be able to exercise this belief during the purchase decision process and the impact of this belief may be observed on the final purchase decision.

Response Costs

The response costs construct represents the time, money, and effort associated with the adoption of protective behavior in the event of a threat. Similarly, the costs incurred from adopting privacy behavior (establishing privacy preferences, adopting privacy education or using a privacy tool) is gauged in terms of time, money, and effort. For instance, establishing privacy preferences

from reading the privacy statements requires time and effort, and an individual must be willing to spend that time and effort to adopt such a privacy behavior.

Research Problem Theory

This section discusses the research question while developing the notion of consumer privacy behavior in the online environment and the purchase decision process. Furthermore, the problem theory is streamlined to focus on consumer privacy behavior during the purchase decision process. Finally, the research model that guides the study is presented.

This study characterizes consumer privacy behavior by establishing privacy preferences, adopting privacy education, and using a privacy testing tool. Privacy preferences and privacy education are explained in the context of general devices. A privacy testing tool is explained with respect to IoT devices.

Privacy preferences allow consumers to be informed on the methods of data collection, storing, and sharing employed by devices in general. This knowledge encourages consumers to disclose personal and sensitive data based on their preferences. Privacy education through online articles, blogs, and forums inform the consumer on the existing privacy issues in devices and applications. A privacy testing tool for IoT devices scans the IoT device and generates a report identifying potential privacy violations, issues, and concerns. To understand privacy behavior towards the purchase of home IoT devices, it is essential to consider privacy behavior in the online environment.

Internet users value online privacy but trade it off for convenience, incentives, and social inclusion (Katell et al., 2016). Another reason for the trade-off is deviation in attitude from stated

preferences and actual behavior (Berendt et al., 2005). The deviation in attitude takes place because the Internet user is strongly attracted to the Internet world or the Internet application to disclose sensitive data. At this point, the ability of information systems to manipulate human cognition is revealed when the users are unable to follow their privacy preferences (Berendt et al., 2005).

The Platform for Privacy Preferences Project (P3P) is a useful tool that notifies Internet users when a website violates their privacy preferences (Berendt et al., 2005). It is also widely used in client-server programs by developers, websites, and other free online information services (Berendt et al., 2005; Cranor, 2002; Vogelsang & Compaine, 2000). Although P3P is useful in online privacy, it has limited usage with respect to highly scalable infrastructures and has failed to become an effective tool (Berendt et al., 2005; Schaub, Balebako, Durity, & Cranor, 2015). Besides P3P, privacy policies also play an important role in understanding privacy preferences.

Privacy policies provide information on the data collection method used by free online information services along with other data and application details (Katell et al., 2016). These policies enable users to establish privacy preferences, rather than help them to verify if their preferences match with that of the application. The following paragraph discusses the notion of privacy preferences in the IoT environment.

IoT systems have multiple users and each user has different privacy preferences (Schaub et al., 2015). For instance, a home monitoring IoT device will collect video data of all members of the household, including guests who visit. In such a case, it is hard to establish privacy preferences with respect to a single person for a home IoT device. Most home IoT devices have small displays with no clear input and output areas; this makes it difficult for the user to read privacy policies on the device (Peppet, 2014). This means the consumer must read these policies from the official IoT device's website or the IoT device's manufacturer website (Peppet, 2014). Similarly, privacy

policies for home IoT devices do not appear on e-commerce websites, including Amazon.com. Thus, not having easy access to privacy policies has many implications: negligence towards reading privacy policies, oblivious to the data collection methods employed by the device, and non-adoption of privacy preferences. Another type of privacy protection measure is discussed in the following paragraph.

Some other privacy enhancement techniques exist for home IoT devices and other IoT systems. These include the SecKit security framework and HPE Fortify on Demand. The SecKit security framework evaluates the IoT device to check for data protection and other security issues (Neisse, Steri, Fovino, & Baldini, 2015). HPE Fortify on Demand provides security checking services and scans IoT devices for vulnerabilities of which privacy issues hold great significance (HP Inc., 2014). These efficient frameworks and services provide formidable reports that explicitly list the vulnerabilities in the devices. However, these frameworks and services are not user-friendly and cannot be used by consumers during their purchase decision process. For instance, HPE Fortify on Demand is a paid service and caters to the needs of IoT solution providers rather than consumers of home IoT devices.

From the above discussion, I argue that a clear lack of easy access to adopt privacy protection measures exists. This prevents consumers from adopting privacy behavior. Next, I consider privacy behavior in an online environment such as online shopping websites.

Online privacy with respect to information provided by online retailers plays a significant role in consumer purchasing behavior (Tsai, Egelman, Cranor, & Acquisti, 2011). In this study, it was noted that privacy information was invisible to consumers and the study concluded that consumers prefer to shop from privacy protected websites where privacy information is easily accessible. Such preferences are exhibited through privacy decision-making. Incomplete privacy

information, deviation in privacy behavior from stated behavior, cost, and effect of privacy behavior affects the privacy decision-making process or rather the adoption of privacy behavior in the online environment (Acquisti & Grossklags, 2005). Deviation in privacy behavior is attributed to cognitive manipulation of the consumer's behavior, which influences the purchase process and as a result the consumer neglects the privacy preferences (Berendt et al., 2005). For instance, the attractive web experience of online shopping sites influences the consumer's purchase decision process, which is the reason for deviation in privacy behavior (Constantinides, 2004). Besides the lack of easy access to privacy protection and the hindrance in adopting privacy behavior due to cognitive manipulation of online environments, inability to adopt privacy protection measures due to lack of skill is an important consideration in the current study.

Adopting privacy behavior in an online environment requires a certain amount of skill and technical knowledge. For instance, in one particular study adults were able to adopt protective behavior in the online environment because they were more efficient in gathering privacy related information when compared to young adolescents (Youn, 2009). The young adolescents, however, admitted that they did not have the necessary skills to engage in protective behavior in an online environment. In another study that investigated users' reaction to disclosure of personal information on mobile applications, security-aware users were more careful and reluctant in giving away personal information when compared to security unaware users (Eling et al., 2016). This shows that individuals with necessary skill and technical knowledge find it easier to exhibit protective behavior because they are confident that the protective behavior will mitigate a threat.

Additionally, if consumers have the capacity to read privacy policies or privacy related articles, establish privacy preferences, verify if their preferences match with that of the device, and engage in privacy education, then they will do so during their purchase decision process.

The above discussion indicates that there are several factors affecting privacy behavior in the online environment during the purchase decision. Similarly, privacy behavior towards home IoT devices too are affected by factors such as time, effort, cognitive manipulation of web experience, and lack of privacy information during the purchase decision process.

Research Model

The research model in Figure 2 guides this study. Although the study followed qualitative research methods, the model helped formulate the interview questions. Constructs from PMT—self-efficacy, response efficacy, and response costs—addressed consumer privacy behavior. From Figure 2, consumer privacy behavior comprises establishing privacy preferences, adopting privacy education, and using a privacy testing tool.

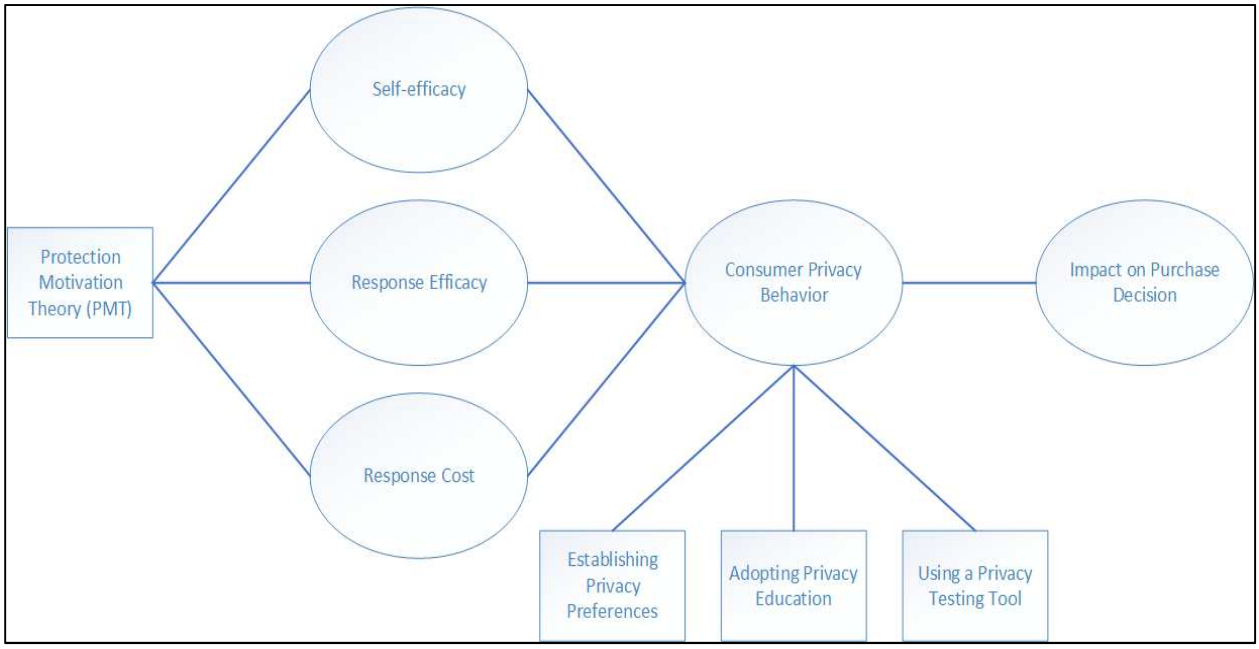

Figure 2: Research model

This model facilitates understanding of the purchase decision process, wherein the influence of self-efficacy, response efficacy, and response costs on consumer privacy behavior is analyzed. The belief in the ability to engage in one of the above-mentioned privacy protection measures is explained by self-efficacy and the belief that the protection measure is able to mitigate a threat is explained by response efficacy. Furthermore, the costs (e.g., money, time, and effort) incurred by indulging in privacy protective behavior is represented by response costs. In the current study, the consumer privacy behavior is analyzed when an individual decides to engage in any one of the protective measures, and the impact on the purchase decision process is also evaluated. This evaluation reveals whether the consumer is inclined towards changing her purchase decision. This change, however, can result in a positive or negative outcome with respect to the purchase of a particular home IoT device.

Conclusion

This chapter explained the implication of PMT and its constructs (self-efficacy, response efficacy, and response costs) on consumer privacy behavior during the purchase decision process.

The section on the research problem theory explained privacy behavior in the online environment and the existing privacy protection measures for home IoT devices along with its limitations. A contrast between online privacy behavior while using free online information services and online privacy behavior during the purchase decision process of home IoT devices-was explained in the research problem theory. Finally, the research model that guided the study was presented and explained.

The next chapter presents the methodology used in the current study.

Chapter 3: Methodology

Introduction

This chapter discusses two data analysis methods employed to analyze different datasets: customer reviews and interview data. Content analysis of customer reviews was performed to primarily understand the purchase decision process for home IoT devices in an online environment and the factors that affect the process. The research model from Chapter 2 guided the qualitative analysis of interview data to understand the impact of self-efficacy, response efficacy, and response costs on consumers' privacy behavior, as well as the consequences of such behavior on the purchase decision process. Privacy behavior constituted the use of three privacy protection measures: establishing privacy preferences, adopting privacy education, and using a privacy tool.

The remainder of the chapter describes the purpose of the employed qualitative research methods, the data analysis procedures adopted for analyzing customer reviews and interview data, and the essential ethical considerations for the research study.

Justification for the Paradigm and Methodology

Qualitative data analysis procedures are very useful in exploratory research. This type of exploratory research was necessary because the baseline knowledge on IoT systems and the surrounding privacy issues with respect to the population of interest was unknown (Brown, Sorrell, McClaren, & Creswell, 2006; Dupuis, 2014).

In past studies, qualitative data analysis of interview data has been employed to understand a consumer's purchase decision process. The method helped discern the shopper's attitude that affects the purchase decision process (Eckman, Damhorst, & Kadolph, 1990). Qualitative research methods were also used to study another aspect of consumer buying behavior: "impulse buying behavior". In this particular study, a consumer's motivation towards impulse buying was analyzed during the purchase decision process (Hausman, 2000).

Consumer buying behavior is affected by many factors, and these factors are analyzed by employing qualitative research methods (Mohr, Webb, & Harris, 2001). One such factor is the impact of a company's social responsibility on consumer buying behavior. Digital and social media are some other factors that influence the consumer's behavior during the purchase decision process (Powers, Advincula, Austin, Graiko, & Snyder, 2012). In summary, there are multiple factors that have the potential to influence the purchase decision process irrespective of the product and this can be studied by employing qualitative research methods.

The current study considers the adoption of privacy behavior during the purchase process. Employing qualitative research methods in this study facilitates an understanding of the possible relationships between consumer privacy behavior and the consumers' purchase decision process with respect to home IoT devices.

Next, I discuss the need for content analysis on customer reviews as it relates to consumer buying behavior during the purchase decision process in the online environment.

Content Analysis of Customer Reviews

The current study analyzes the impact of consumer privacy behavior on the purchase decision process using unobtrusive observation methods. This method was implemented on

publicly available information, which consisted of customer reviews of smart home IoT devices on the Amazon.com website. It provided insight into consumers' shopping behavior, which was analyzed by reviewing the posted comments and reviews on e-commerce websites such as Amazon.com. This process highlighted several aspects of consumer privacy behavior during the purchase decision process. A detailed description on these insights is provided in chapters four and five.

E-commerce websites serve as an effective platform for observing consumer buying behavior. Customer reviews contain vast amounts of information on the product and express the feelings or emotions of consumers. Customer feelings and emotions are exhibited through the two dimensions of customer reviews: comments and ratings. These dimensions are essential considerations in this study as they help to understand the purchase decision process.

Online reviews on e-commerce websites provide useful information to other consumers. The usefulness or helpfulness of these reviews is determined in part by length; lengthier reviews or in-depth reviews are more helpful to consumers when compared to shorter reviews (Mudambi & Schuff, 2010). These reviews decrease uncertainty, which in turn increases a consumer's confidence in the product. However, this is time-consuming because the consumer is required to read multiple reviews to be convinced of her purchase choice (Mudambi & Schuff, 2010). Reviews and ratings possess extremity: positive, negative, or neutral. These extremity conditions are symbolic to a consumer's attitude in an online environment such as an e-commerce website (Mudambi & Schuff, 2010).

Customer attitude or behavior is reflected through complaints and compliments provided in the reviews and these reviews in turn help the reader in the purchase decision (Yang & Peterson, 2004). Content analysis of customer reviews provide in-depth knowledge on customer satisfaction,

customer loyalty, and perceived value, which are key determinants of the customer behavior in online services (Yang & Peterson, 2004). Therefore, content analysis of customer reviews is an unobtrusive observation that allows market researchers to understand customer buying behavior (Kozinets, 2002). The advantage of this type of observation is that consumer buying behavior and their interactions with other components of the online environment are observed without disturbing them in their natural setting (Jacoby, 1978).

Ratings and reviews have the potential to define the success or failure of a product because they influence the buying behavior of customers (Connors, Mudambi, & Schuff, 2011). Reviews reflect an individual's opinion and this impacts the quality dimensions of online services and information systems. Through the insights from the analysis of customer reviews, businesses can improve their processes and technologies (Yang & Fang, 2004). For instance, a customer's perceived ease of use (a construct from TAM) towards a particular information system is measured by the minimum level of effort a consumer exercises to ensure that the system is fully functioning (Yang & Fang, 2004). This is reflected in the reviews of different consumers. This process of writing reviews defines end-user satisfaction through which businesses make corrective decisions and propose new ways of improvement (Yang & Fang, 2004).

This section explained the importance of content analysis of customer reviews within the online environment. It also highlighted the significant aspects of consumers' purchase behavior under the influence of external factors that affect businesses.

The following section details the research procedures used in the current study.

Research Procedure

Data Collection Process of Customer Reviews

Five hundred customer reviews of the top 10 smart home IoT devices were collected from the Amazon.com website. The selection criteria for these top 10 devices was based on Gartner's listing of smart home sub-categories ("Gartner Says Smart Cities Will Use 1.6 Billion Connected Things in 2016," 2015) and Amazon's best sellers in the smart home category.

The customer reviews of verified purchases were grouped based on two categories: rating scale and review groups. The rating scale ranged from 1 to 5 and the review groups consisted of top reviews and recent reviews. The 500 reviews were equally divided among the 10 devices based on the abovementioned categories. Fifty reviews were collected for each of the 10 devices. The equal distribution and grouping of reviews for one device is represented in a factorial format in Table 2. This grouping and distribution was replicated for the remaining nine home IoT devices.

Table 2: Factorial distribution of customer reviews for a home IoT device

Ratings		**R1**	**R2**	**R3**	**R4**	**R5**
Reviews	**Top**	(R1, top) N = 5	(R2, top) N = 5	(R3, top) N = 5	(R4, top) N = 5	(R5, top) N = 5
	Recent	(R1, recent) N = 5	(R2, recent) N = 5	(R3, recent) N = 5	(R4, recent) N = 5	(R5, recent) N = 5
Total number of reviews (N = 50)		N = 10	N = 10	N =10	N = 10	N = 10

Content Analysis of Customer Reviews

The content analysis of customer reviews was performed by employing the method suggested by Stambor, Z (Z, 2005).

The large dataset of customer reviews was coded by employing appropriate qualitative data analysis procedures. First, a thorough reading of the 500 reviews was performed and a coding scheme with six major themes was developed along with several sub-themes. Each of the themes contained an operational definition that clearly explained the meaning of the theme. The units of measurement for the customer review dataset comprised of words, phrases and sentences. Table 3 displays the format used to analyze the narratives within the reviews.

Table 3: Format for analyzing customer review narratives

Categories	Operational Definitions	Unit of Measurement
1. Need for the device • Comfort • Security/reliability • Convenience • Useful • Easy to use • Improves individual's performance	Explains why an individual needs the device.	Phrases, words, sentences
2. Features • Performance • Functionalities • Customer service help • Storage capacity	Explains the purpose for which the device was built.	
3. Security • Anti-malware software and automatic upgrades • Safe from spying • Protection from DDoS attacks • Voice/touch authentication		
4. Privacy • Secure methods of data collection/transfer/sharing		

• De-identifying of data • User consent before data sharing • Protection of PII • Privacy preferences • Privacy tools • Education on privacy		
5. Cost • Ease of use/installation • Free from effort • Time • Money		
6. Integration with other devices • Types of devices it connects to • How easy is it to connect? • Needed workarounds with existing devices/things to maximize usage of device • Are those connected devices popular ones?		

This format was followed while analyzing the reviews. The content from the reviews was categorized into the six themes listed in the table above, and effective coding strategies were applied to analyze the data. A well-structured explanation of observed trends was developed through this process and is presented in the next chapter.

Data Collection Process of Interview Data

Semi-structured interviews were conducted among 18 university students. The participants were selected and recruited using flyers posted around campus. During the recruiting process, participants were asked to fill out a qualifying survey. Some of the survey questions related to gender, age, major, and ethnicity. Participants were selected based in part on major and this was done to ensure a balance between students with a computer science background and those without a computer science background.

Participants were notified through a scheduling system that provided details on the time and place of the interview sessions. These sessions were conducted over two weeks. The study participants were initially introduced to the research team and were then asked to read a consent form and sign if they were in agreement.

The interview sessions lasted between 20 and 30 minutes in duration. The questions in the interview sessions focused on consumer privacy behavior during the purchase decision process, baseline knowledge on privacy issues, privacy protection measures in smart home IoT devices, and impact of consumer privacy behavior on purchase decisions. Table 4 provides a list of sample questions from the interview sessions.

Table 4: Sample questions from the interview sessions

Topic	Sample Question
Purchase Decision Process	Describe the research process you follow while making purchase decision for home IoT devices?
Baseline Knowledge on privacy issues	What are your thoughts and impressions after reading the HP article? What level of understanding do you have on privacy issues or concerns as it relates to home IoT devices?
Privacy Preferences	What are some of your privacy preferences in relation to the collection of sensitive or private data by the home IoT device?
Privacy Education	What are the online resources you refer to; and what type of information on privacy issues do you look for in these resources?
Privacy Testing Tool	How inclined are you towards using a privacy testing tool?
Purchase Decision	How much do you see yourself implementing these privacy protection measures during your research process? Do you think these measures have an impact on your purchase decision of the device?

Because there was a discrepancy in understanding the definition of smart home IoT devices and privacy issues in these devices, articles were handed out to the participants to address this discrepancy. These articles were sections from a published report, “A HP study on IoT security”,

released by the Hewlett Packard company. They informed participants on existing privacy issues in home security IoT devices and other security related issues. This helped the participants to convey their thoughts and impressions, and establish their baseline knowledge on data collection methods in IoT systems, among other privacy issues. The clippings from the HP report are presented in Appendix A.

At the end of the interview session, study participants were compensated with a $20 Amazon gift card for their time and participation. The interview sessions were recorded using a digital voice recorder and later transcribed. Confidentiality of the participants' identity was maintained by not disclosing their names and personal details from the demographic survey and the interview sessions.

Data Analysis Process of Interview Data

The coding strategy for analyzing the interview data was developed based on the methodology suggested by Brown et al. (Brown et al., 2006). The first step in the coding strategy involved a thorough reading of the interview data followed by the generation of significant statements. The significant statements were further analyzed and overlapping statements were removed to generate more concrete ideas, which resulted in the development of invariant structures or constituents. These invariant structures were classified into nine major themes. These nine major themes were developed based on the research model and from performing a thorough reading of the transcripts.

With the help of the invariant structures, meaning units were inferred by rightly discerning the meaning of the verbatim statements of the study participants. These invariant structures were categorized into five major themes (the nine major themes were reduced to five major themes to reconcile the differences among the meaning units). The invariant structures along with their

meaning units were compared and studied for the entire interview dataset. The steps involved in the generation of major themes is illustrated in Figure 3. The insights from the five major themes are discussed in detail along with their implications on the research problem in Chapter 4.

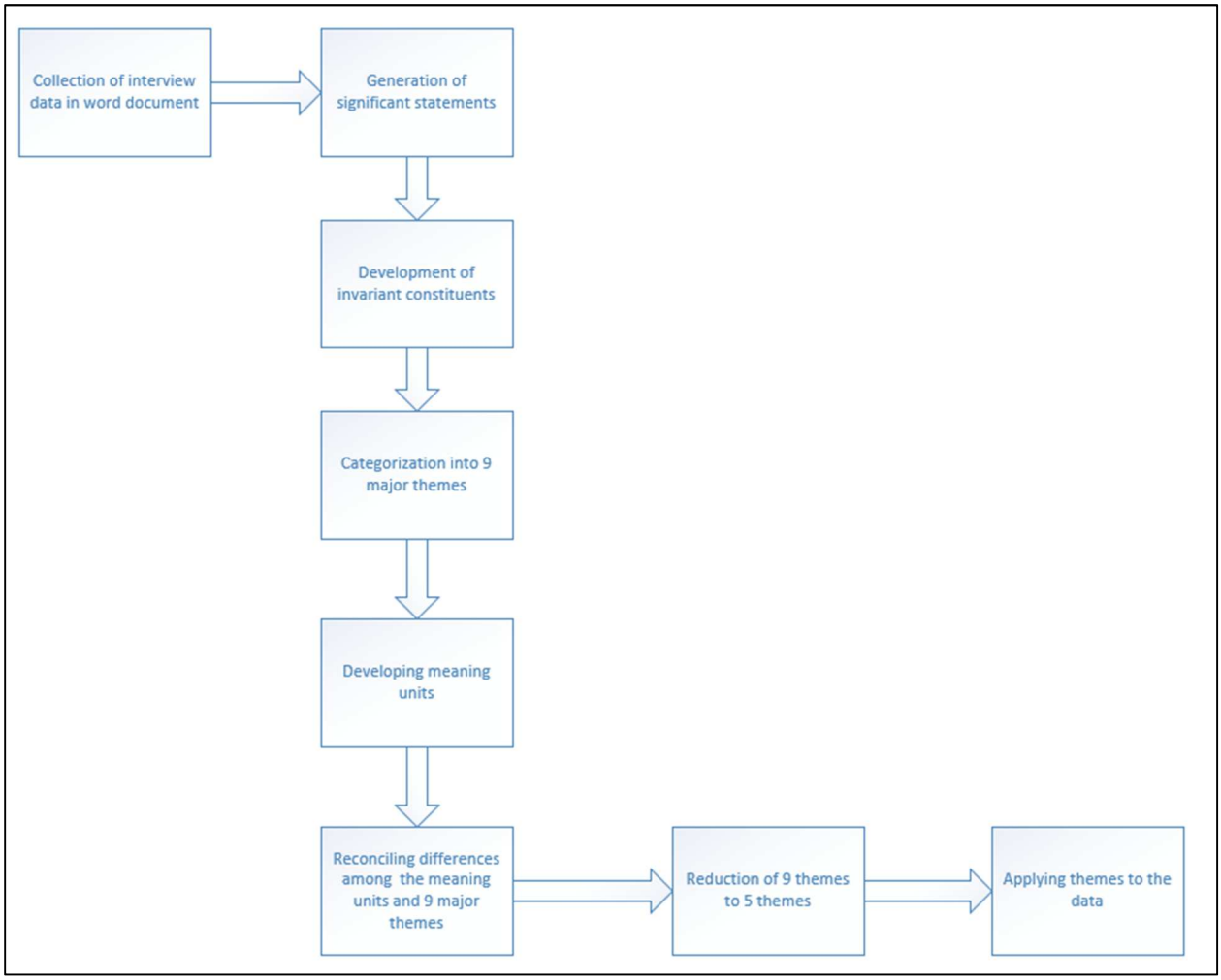

Figure 3: Coding scheme strategy

Ethical Considerations

Since human participants were involved in this study, it was important to consider any potential risks that maybe associated with their participation in this research. In accordance with

this perspective, participants were informed of the study's purpose and could stop or leave the interview session if they did not want to continue at any time. The participants were compensated with a $20 Amazon gift card for their time and participation.

The University of Washington Human Subjects Division granted exempt status for this study under the IRB ID: STUDY00001326.

Conclusion

This chapter explained in detail the justifications for the employed research procedures, followed by an explanation on the qualitative data analysis processes of customer reviews and interview data. Finally, it also discussed the ethical considerations towards human subjects. In the next chapter, I discuss the results of this study.

Chapter 4: Analysis of Data

Introduction

This chapter discusses the results obtained from the two data analysis phases: qualitative analysis of customer reviews and interview data. The research model described in Chapter 2 guided the major themes developed during the analysis phases. The overarching themes helped in the understanding of consumers' privacy behavior during the purchase decision process. Constructs such as self-efficacy, response efficacy, and response costs from PMT were considered external factors that affect a consumer's privacy behavior during their purchase decision process. This is demonstrated through the results gathered from the two data analysis procedures.

In this chapter the results from the two data analysis processes is presented followed by concluding remarks based on the research model and the research problem as discussed in Chapter 2 of this report.

Patterns of Data for Each Research Issue

This section details the insights that were obtained from the data analysis processes of customer reviews and interview data. First, the results of the content analysis phase are provided, followed by the results from the qualitative data analysis of interview data. The results from these two phases are guided by the research model presented in Chapter 2.

Content Analysis of Customer Reviews

The customer reviews collected from the Amazon.com website provided insights into the purchase decision process of online shoppers. The website served as an effective platform to understand consumer privacy behavior from the customer reviews and comments.

The information in the reviews indicated several factors that influence a consumer's purchase decision. The major themes that emerged from coding the customer reviews were need, cost, features, ease of use, usefulness, convenience, comfort, privacy, security, and integration with other devices. The primary concern of most consumers revolved around constructs from TAM, such as ease of use and usefulness of smart home IoT devices.

The goal of a majority of consumers is to possess the ability to efficiently set up the device and ensure proper integration with other home automation equipment. To achieve this goal, consumers look for specific information on installation instructions in reviews or seek help from customer service help lines. The videos and pictures in the reviews that display the device working are useful resources that increase the device's perceived ease of use. Many customer reviews highlighted that the device's reliability is of top concern apart from its ability to connect to other home automation equipment. The reliability of the device was directly associated with usefulness of the device by many consumers.

From the 500 reviews, only six reviews showed a clear concern towards privacy issues in smart home IoT devices. All six reviews either discussed privacy issues in the home IoT device or expressed concern over the issue. However, five reviews indicated that the device was not returned despite raising concern over the issues.

Five out of the six reviews were categorized as "top reviews" by the website. Top reviews are those voted as most helpful reviews by other consumers interested in the same device as the writer of the top review. This is a possible indication that consumers considered those reviews important and helpful to some degree and did not ignore them completely. In other words, if consumers ignored these reviews, they could not have appeared in the "top review" category. However, the five top reviews also included issues relating to cost, features, functionality, integration to other devices, among other issues. This means there could have been some other information that was of interest to the reader that prompted her to vote the review as 'helpful'. Additionally, some of the reviews that contained detailed concerns over privacy issues suggested that the writers may have prior technical knowledge that helped them write about privacy issues as it relates to network technologies. Most of these privacy issues related to video data collected by home monitoring systems with IP traceable web cams.

The next section provides the results from the qualitative data analysis phase of interview data.

Qualitative Analysis of Interview Data

In this section, a detailed explanation of the insights gathered from the five major themes generated from the coding scheme strategy in chapter three is provided.

1. Purchase Decision Process

The purchase decision process constitutes the steps a consumer takes towards the purchase of a product. This process was evaluated for two types of products: daily necessity items (e.g., food, clothing, essential electronic devices, books, etc.) and home IoT devices (e.g., Alexa, Nest thermostat, indoor cameras, etc.). The evaluation was performed to understand the difference

between the two processes. Every consumer follows a certain type of research process before buying a product. The process, however, varies among consumers and products.

Most participants identified similar research processes for daily necessity items and smart home IoT devices. Cost, reviews, shipping rates, features, functionality, and need for the device were the overarching subthemes that emerged from the narrative description of their research process. In the following paragraphs, the subthemes are explained.

Comparing prices on different websites was another important aspect that constituted the purchase decision process for most participants. Product prices were compared across a wide range of websites and price drops were key indicators that influenced their purchase decision. Besides product price, shipping cost was of great concern to many participants and an important deciding factor during the purchase decision process. Many participants were drawn to purchase products when the shipping rates were low or absent. Elaborate descriptions on information such as shipping rate and product cost was easily found in reviews written by other consumers.

Reading and analyzing reviews was an important step in the research process for most participants. Reviews provided information on product description, functionality, features, pictures of the device, and video tutorials on how-to-use the device. The most useful reviews were found on reputable sites such as Amazon, Google, and Reddit. These reviews were also critically analyzed and relevant information was gathered to make wise decisions on the product. For instance, one participant bought a home IoT device with adequate features based on need, thereby avoiding spending money on extra and unnecessary features.

Along with reviews, ratings on a product also play a crucial role in the purchase decision process. It is an integral part of the process because many participants said that it gave them

significant insight into the level of confidence other consumers showed towards a particular product. Reviews and ratings facilitated the 'cost-benefit analysis' participants would engage in when making a purchasing decision. By doing this, they could evaluate the product based on cost and need.

In conclusion, considering privacy issues or adopting privacy behavior during the purchase decision process was not a prominent practice among most participants. The few participants who incorporated privacy behavior had a good baseline knowledge on cybersecurity in information systems. Most participants were not aware of these issues and did not express any concern towards them. Additionally, they did not consider it necessary to incorporate or address these issues during their purchase decision process.

2. Need

The need for a smart home IoT device is characterized by convenience, lifestyle, comfort, and cost. However, the need varied among participants; some recognized an immediate need for it, while others recognized a future need or no need at all. The convenience aspect of smart home IoT devices fascinated many participants but their fascination often did not overrule their lack of need for it. The constraints that govern the need for a device were cost, lack of space to set up the device, and privacy issues. For instance, one participant was reluctant in investing in a home IoT device and was even willing to wait for companies to resolve the prevailing privacy issues in them before he would consider buying it. Most participants who expressed a future need for a home IoT device agreed that these devices create a convenient and comfortable lifestyle. They also mentioned that these devices help them save energy and household utility costs.

Some participants also expressed interest in keeping up with new technology by investing in home IoT devices and they were excited to explore the features and functionality in them. Some others were more interested in building such devices on their own to pursue personal intellectual challenges.

3. Privacy Issues or Concerns

Privacy issues in home IoT devices revolve around collecting, storing, and transferring video, audio, and sensitive data among the different components of the IoT infrastructure. Baseline knowledge on these issues was established among participants with the help of a report released by the Hewlett Packard company. Some participants did not have prior knowledge on privacy issues and therefore the report was very useful and helped them understand the various aspects of privacy issues in home IoT devices. On the other hand, some participants had a good understanding of the existing privacy issues in these devices and did not read the report.

The questions that followed the reading of the report assessed the participant's baseline knowledge on privacy issues. The thoughts and impressions of the participants clearly showed that most of them were concerned with being constantly monitored by home monitoring IoT devices.

Participants also felt they had the right to know what the company does with their photos, video, audio, and sensitive data. Many responses exhibited a great need for securing private data to preserve their anonymous identities on other websites. A few others felt it was reasonable for companies to collect data and do as they pleased because the participants felt they could not do nothing to prevent it. Still others felt their information is not "top secret" and therefore were not concerned with the consequences of privacy violations in home IoT devices. In some cases, participants felt the privacy issues did not outweigh the benefits provided by these devices.

Besides the abovementioned trends in data, two other subthemes emerged: participant's reaction to the type of data collected and trust in the company manufacturing the home IoT device. The two types of data collected by home IoT devices are sensitive data (personally identifiable information, audio, and video files) and non-sensitive data. All participants preferred their sensitive data to be well secured within the IoT infrastructure. Secure collection, storing, and transferring of video data files were of top concern for most participants. In one case, the participant approved the process of collecting, storing, transferring, and analyzing sensor data of home IoT devices so long as they were destroyed at the end of the process. In another case, a participant prefers to turn off the home monitoring system when it's not in use to prevent unnecessary video leakage that may occur on the Internet. Devices that collect temperature data of the home were less of a concern to participants when compared to home monitoring systems that collect video and audio data files.

Some participants evaluated the data collection process by employing a "cost–benefit analysis". For instance, if sensitive data of a consumer is required by the device for a particular feature to function, then the participant would provide that data to leverage the benefit despite the potential consequence of doing so.

In addition to participants' reaction to the type of data collected, consumer trust in the manufacturing company was an important consideration for many participants. Some participants expected reputable companies to securely manage sensitive data collected by the home IoT device. Participants also were interested in checking a company's track record of maintaining user privacy and its ability to produce secure devices that ensure consumers' privacy protection. Some other participants also expressed interest in investing in products from reputable companies because

such companies provided monetary compensation in the event that a consumer becomes a victim of a cyberattack due to misuse of sensitive data on the Internet.

4. Privacy Protection Measures

Three privacy protection measures were discussed in the interview sessions with participants: establishing privacy preferences, adopting privacy education, and using a privacy testing tool. Participant responses to these three measures were recorded and the following inferences made.

Most of the insights in this theme were similar to those in theme three, "participant's reaction to the type of collected data". Most participants had preferences in the way video data files were collected, stored, and transferred. Devices that performed video and audio recording without permission were unacceptable to the participants. They also expected companies to maintain transparency in data collection, sharing, and storing. Enabling privacy settings and reading policies on audio and video recording methods were recognized as good practices of establishing privacy preferences; however, they were difficult to use or follow. Besides the few who denied having any privacy preferences for no specific reason, there were many others who realized the difficulty in establishing privacy preferences during the purchase decision process. There were also a few participants who expressed interest in ensuring their privacy preferences matched with that of the smart home IoT device they were going to buy.

Privacy education is the process through which a consumer is constantly updated on existing privacy issues in IoT devices from various online resources such as blogs, reviews, forums and online articles. All participants exhibited an inclination towards reading reviews and articles from blogs, forums, and websites such as Amazon, Google, and Reddit. For some, reading reviews

and articles on privacy issues on these devices was a “habit”. Some responses also highlighted that the cost associated with privacy education is high and would rather avoid it. While some others suggested that gathering information from technically sound peers was also a good method in privacy education rather than reading articles and reviews.

The use of a privacy testing tool was a new method for all participants, but when the idea of using one was suggested, some participants expressed their interest in trying it. Some said the tool might increase their confidence in the smart home IoT device they were buying. If it was a new tool with no track record of success, however, the participant would decline using it. Some participants said they would use the tool only if the documentation was easy to follow and the download was easy to perform. Some other participants were concerned about the company that built the tool, level of bias, reliability, and accuracy of the tool.

5. Impact on Purchase Decision Process

The two primary areas of focus in this theme are ability to implement privacy protection measures in the purchase decision process and the impact of privacy protection measures on the purchase decision.

Most participants were confident that privacy protection measures would have a significant impact on their purchase decision. Many said that taking privacy protection measures seriously is time-consuming and requires much effort. However, some participants considered it convenient to have privacy protection measures in the form of “easy click buttons.” On clicking these buttons, information on privacy issues or privacy protection measures can be generated. However, they also admitted that it is very unlikely for companies to take such a large initiative towards resolving privacy issues. Some said this might make the product popular but it hampers the sales pitch of the

device. For many participants, initiatives towards privacy concerns were of utmost importance when compared to the brand or popularity of the device. They were comfortable switching to other products and brands that emphasized or embraced privacy concerns of consumers. Finally, adoption of privacy protection measures in the purchase decision process is worthwhile because of the large investment associated with the purchase of home IoT devices.

The following section contains concluding remarks for the two data analysis phases in relation to the research problem discussed in chapter two.

Conclusions for Each Research Issue or Proposition

This study employed qualitative research methods for two data sets: customer reviews and interview data. The findings from these two data analysis procedures are explained in the following sections.

Content Analysis of Customer Reviews

The content analysis of customer reviews provided in-depth insight into consumers' purchase decision process in the online environment. Most of the issues discussed in the reviews revolved around customer satisfaction problems. The few reviews that raised privacy concerns about the device were verified purchases indicating the consumer bought the device despite the noted concerns.

The content analysis procedure indicated aspects of consumer buying behavior that affect the purchase decision process. For instance, defective devices upset consumers and negative feelings were expressed in the reviews. Although the analysis procedure explained some possible issues of customer satisfaction that could be directly associated with consumer buying behavior,

very little could be inferred on consumer privacy behavior. Consumer privacy behavior in relation to establishing privacy preferences, adopting privacy education and using a privacy testing tool, was difficult to understand. However, qualitative analysis of interview data clarified the impact of PMT's constructs on privacy behavior and its consequence on a consumer's purchase decision.

Qualitative Analysis of Interview Data

Privacy issues in smart home IoT devices are a great limitation to the IoT ecosystem. The concern towards resolving these issues is a never-ending battle for both consumers and companies. Adopting privacy protection measures paves a way for improvement in resolving the privacy issues; but convenience slows down the improvement process because consumers find it almost impossible to give up convenient lifestyles. Most discussions with the study participants highlighted a great level of ambiguity in deciding whether privacy concerns or convenient lifestyles hold more value.

Despite this ambiguity, there was a clear line of thought that emerged. Most participants showed a great deal of interest in discussing privacy issues in smart home IoT devices after reading the HP article. Some even initiate conversations on privacy issues with peers. They also highlighted that the insights from the conversations altered their regular purchase decision process. The progressive method of knowledge gathering increases awareness on prevalent privacy issues. This progressive thinking may lead consumers into considering these issues with greater seriousness and not give into decisions based on convenience.

The purchase decision process is the only phase during which a consumer's behavior or attitude towards a product is evaluated. The interplay of factors such as convenience, cost, status quo, and education level, is well exhibited during the purchase decision process. However, it is difficult to predict which one of them overpowers the other. It is more difficult to understand the

relationship of each one of them with a consumer's purchase decision. In this study's analysis, these factors have been considered side by side to determine their impact on a consumer's purchase decision.

The purchase decision process is almost the same for most products and devices. The time duration of the process and the type of information a consumer looks for varies. Consumers look for product information on familiar online resources. It was very unlikely for them to explore new online resources during their purchase decision process as it requires time, effort and technical skill. This explains why consumers with good background knowledge on IoT and the related privacy issues were quick to highlight the "extra steps" they took to ensure privacy protection during the narrative description of their purchase decision process. These extra steps did not emerge instantly; keeping up with technology news in general is an ongoing process. The same can be applied to acquiring knowledge on privacy issues in smart home IoT devices. It is challenging for consumers to find credible online resources that can educate them on privacy protection and help them make wise purchase decisions at the same time.

Adopting privacy protection measures for smart home IoT devices is not as common as the cost–benefit analysis method that consumers adopt during their purchase decision process. The cost–benefit analysis method was used to compare entities such as price, features, and functionality of a device. Among the three privacy protection measures, adopting privacy education was fairly easy to perform when compared to establishing privacy preferences or using a privacy testing tool. The easy accessibility to online resources that provide one of the three protection measures is difficult to obtain. However, during the study when information on privacy issues was easily made available through hand distribution of articles, most participants exhibited a strong inclination

towards discussing the issues. This inclination has a large impact in the way consumers make their purchase decisions.

Conclusion

The data analysis procedures were employed for analyzing customer reviews and interview data. The content analysis of customer reviews contributed to the understanding of the purchase decision process. In addition, it highlighted the factors that affect the purchase process and most of these factors relate to customer satisfaction. The reviews and ratings were reflective of a consumer's attitude towards a particular device. Positive and negative feelings towards a device were highlighted in the reviews and this provided insight into a consumer's attitude during the purchase decision process.

The coding and subsequent analysis of interview data provided useful insights into consumers' privacy behavior. Establishing privacy preferences, adopting privacy education, and using a privacy testing tool characterize privacy behavior. Participant responses to the abovementioned privacy protection measures highlighted several factors that impact the consumer's privacy behavior and their purchase decision process. Many of the factors corresponded with the constructs of PMT.

In the final chapter, I discuss issues in the research methods used and results, followed by implications, limitations, and future work.

Chapter 5: Conclusions and Implications

Introduction

In this study, the impact of consumer privacy behavior on the purchase decision process was examined. Three constructs from PMT—self-efficacy, response efficacy, and response costs—were studied in relation to the adoption of privacy protection measures that cultivate consumer privacy behavior. The three privacy protection measures were: establishing privacy preferences, adopting privacy education, and using a privacy testing tool. Qualitative research methods were employed to understand consumer privacy behavior and evaluate its impact on the purchase decision process.

The content analysis of customer reviews provided useful insight and also facilitated an understanding of the factors that influence the purchase process of home IoT devices. Additionally, it contributed very little to the assessment of the consumer's baseline knowledge of home IoT systems and the surrounding privacy issues.

The qualitative analysis of interview data provided in-depth knowledge into consumer privacy behavior. It also accounted for the factors that affect the purchase decision process as observed in the content analysis phase.

This chapter discusses the possible limitations of using qualitative research methods, followed by the conclusion and future work.

Conclusions about the Research Problem

The results from the qualitative data analysis process highlighted multiple factors that govern the purchase decision process. Although these factors did not directly relate to a consumer's privacy behavior, they were reviewed in light of self-efficacy, response efficacy, and response costs. The content analysis of customer reviews exhibited very little or no inclination towards addressing privacy issues in home IoT devices during the purchase decision process. Similarly, the qualitative analysis of interview data revealed that participants were somewhat inclined towards considering privacy issues prior to making a purchase. The participants of the interview session who had prior knowledge on IoT systems and its surrounding challenges, were quick to acknowledge their desire to address the privacy issues and indicated its impact on their purchase decision. The same was observed while discussing the privacy protection measures.

The insights from this study possess great potential for application in the real world and some of these are discussed in the future work section.

Limitations

This study does have some limitations worth noting. First, this study does not use software tools to perform sentiment analysis of customer reviews. Sentiment analysis tools help the researcher gauge the feelings of review writers and this could be useful in understanding the possible intentions or motives of the writers as it relates to privacy concerns and issues. Second, since a single coder was involved in the qualitative analysis phase, there could be certain shortcomings in the analysis of data. Third, the analysis of reviews on Amazon.com is limited in the insight it provides into the purchase decision making process since presumably most people

that leave a review have already made the purchase. The use of interviews helped mitigate this limitation. Fourth, participants could have made statements consistent with what they thought the interviewer wanted to hear. While several methodologies are susceptible to satisficing, it is something that must nonetheless be considered. Finally, nothing was empirically tested in this study. In the methods employed, we cannot test for causation or even correlations. Regardless, significant insight was gained despite these limitations.

Further Research

Finally, this section discusses future research in relation to the limitations mentioned in the previous section. First, the use of quantitative data analysis procedures to test the research model in chapter two may help compensate for any limitations inherent in a strictly qualitative approach.

Additionally, an experimental study could be conducted on participants to observe their purchase decision process for products in general and home IoT devices in particular. The experiment must focus on ensuring easy access to privacy protection measures as this facilitates a deeper understanding of consumer privacy behavior during the purchase decision process. For instance, a pilot website that emulates the features of an e-commerce website, such as the Amazon.com website, could be developed. Besides these features, links or attachments to online resources that provide privacy education maybe provided in the product description area. The goal of this experiment would be to validate the impact of easy access to privacy protection measures on the purchase decision process.

Conclusion

This study contributes to the body of knowledge as it pertains to understanding the impact of consumer privacy behavior on the purchase decision process of smart home IoT devices. In the current study, establishing privacy preferences, adopting privacy education, and using a privacy testing tool characterize consumer privacy behavior. These privacy protection measures are necessary to address privacy issues in home IoT devices. The purchase decision process is a good place to begin with as it provides in-depth understanding into a consumer's purchase behavior. This study helps inform us on the factors that affect a consumer's purchase choice and the influence of self-efficacy, response efficacy, and response costs on the consumers' privacy behavior. This study also helps inform us on the lack of easy access to privacy protection measures being the primary cause for privacy trade-offs with convenient purchase choices. This consequently leads to the notion that consumers can be inclined towards privacy behavior during the purchase decision process if privacy behavior is easy to adopt. This inclination might have an impact on the consumer's purchase decision and ultimately the sale of home IoT devices.

When businesses begin to embrace this school of thought, they will be driven to instill trust in their consumers to assure themselves of sustainable business growth. This implies businesses need to adopt disruptive innovation to explore the possibility of a sustained and profitable IoT business. Disruptive innovation in this context means that companies must begin investing in privacy protection measures despite it being a threat to the business. Different businesses that have adopted disruptive innovation have compared their successes with that of incumbent businesses that neglect disruptive innovation (Christensen, Raynor, & McDonald, 2015). Similarly, there is great potential in embracing disruptive innovation to improve the business of home IoT devices, especially through e-commerce platforms.

Bibliography

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security Privacy*, *3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613–643.

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

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-Commerce: Stated Preferences vs. Actual Behavior. *Commun. ACM*, *48*(4), 101–106. https://doi.org/10.1145/1053291.1053295

Brown, J., Sorrell, J. H., McClaren, J., & Creswell, J. W. (2006). Waiting for a Liver Transplant. *Qualitative Health Research*, *16*(1), 119–136. https://doi.org/10.1177/1049732305284011

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523–548.

Camhi, J., & Greenough, J. (2016, August 29). Here are IoT trends that will change the way businesses, governments, and consumers interact with the world. Retrieved May 27, 2017, from http://www.businessinsider.com/top-internet-of-things-trends-2016-1

Carol Wan, & Don Low. (2013). *Capturing Next Generation Smart Home Users with Digital Home*. Retrieved from http://www1.huawei.com/en/static/HW-275915.pdf

Christensen, C. M., Raynor, M. E., & McDonald, R. (2015, December 1). What Is Disruptive Innovation? Retrieved May 24, 2017, from https://hbr.org/2015/12/what-is-disruptive-innovation

Connors, L., Mudambi, S. M., & Schuff, D. (2011). Is It the Review or the Reviewer? a Multi-Method Approach to Determine the Antecedents of Online Review Helpfulness. In *2011 44th Hawaii International Conference on System Sciences* (pp. 1–10). https://doi.org/10.1109/HICSS.2011.260

Constantinides, E. (2004). Influencing the online consumer's behavior: the Web experience. *Internet Research*, *14*(2), 111–126. https://doi.org/10.1108/10662240410530835

Cranor, L. (2002). *Web Privacy with P3P*. O'Reilly Media, Inc.

Dupuis, M. J. (2014). *The Role of Trait Affect in the Information Security Behavior of Home Users*. Retrieved from https://digital.lib.washington.edu/researchworks/handle/1773/26407

Eckman, M., Damhorst, M. L., & Kadolph, S. J. (1990). Toward a Model of the In-Store Purchase Decision Process: Consumer Use of Criteria for Evaluating Women's Apparel. *Clothing and Textiles Research Journal*, *8*(2), 13–22. https://doi.org/10.1177/0887302X9000800202

Eling, N., Rasthofer, S., Kolhagen, M., Bodden, E., Buxmann, P., undefined, … undefined. (2016). Investigating Users' Reaction to Fine-Grained Data Requests: A Market Experiment. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 3666–3675). Los Alamitos, CA, USA: IEEE Computer Society. https://doi.org/10.1109/HICSS.2016.458

Evans, D. (2011). The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. In *Cisco Internet Business Solutions Group (IBSG)*. Retrieved from http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Gartner Says Smart Cities Will Use 1.6 Billion Connected Things in 2016. (2015, December 7). Retrieved February 15, 2017, from http://www.gartner.com/newsroom/id/3175418

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. https://doi.org/10.1016/j.future.2013.01.010

Hausman, A. (2000). A multi-method investigation of consumer motivations in impulse buying behavior. *Journal of Consumer Marketing*, *17*(5), 403–426. https://doi.org/10.1108/07363760010341045

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

HP Inc., H. (2014, July 29). HP News - HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. Retrieved May 22, 2017, from http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WSJj5mjyvIU

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

In, L. (2017). *The Internet of Things in the Modern Business Environment*. IGI Global.

Jacoby, J. (1978). Consumer Research: A State of the Art Review. *Journal of Marketing*, *42*(2), 87–96. https://doi.org/10.2307/1249890

Katell, M. A., Mishra, S. R., & Scaff, L. (2016). A Fair Exchange: Exploring How Online Privacy is Valued. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 1881–1890). https://doi.org/10.1109/HICSS.2016.239

Koufaris, M. (2002). Applying the Technology Acceptance Model and Flow Theory to Online Consumer Behavior. *Information Systems Research*, *13*(2), 205–223.

Kozinets, R. V. (2002). The Field Behind the Screen: Using Netnography for Marketing Research in Online Communities. *Journal of Marketing Research*, *39*(1), 61–72. https://doi.org/10.1509/jmkr.39.1.61.18935

Lestable, T. (2012, March). *Supelec M2M, IoT course 1 - introduction part 2 - 2012*. Technology. Retrieved from https://www.slideshare.net/titidelparis/supelec-m2m-iot-course-1-introduction-part-2-2012

Matt, C., Peckelsen, P., undefined, undefined, undefined, & undefined. (2016). Sweet Idleness, but Why? How Cognitive Factors and Personality Traits Affect Privacy-Protective Behavior. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4832–4841). Los Alamitos, CA, USA: IEEE Computer Society. https://doi.org/10.1109/HICSS.2016.599

McGrath, M. J., & Scanaill, C. N. (2013). *Sensor Technologies: Healthcare, Wellness and Environmental Applications*. Apress.

Mohr, L. A., Webb, D. J., & Harris, K. E. (2001). Do Consumers Expect Companies to be Socially Responsible? The Impact of Corporate Social Responsibility on Buying Behavior. *Journal of Consumer Affairs*, *35*(1), 45–72. https://doi.org/10.1111/j.1745-6606.2001.tb00102.x

Mudambi, S. M., & Schuff, D. (2010). *What Makes a Helpful Review? A Study of Customer Reviews on Amazon.com* (SSRN Scholarly Paper No. ID 2175066). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2175066

Murray, K. B. (1991). A Test of Services Marketing Theory: Consumer Information Acquisition Activities. *Journal of Marketing*, *55*(1), 10–25. https://doi.org/10.2307/1252200

Neisse, R., Steri, G., Fovino, I. N., & Baldini, G. (2015). SecKit: A Model-based Security Toolkit for the Internet of Things. *Computers & Security*, *54*, 60–76. https://doi.org/10.1016/j.cose.2015.06.002

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. In M. Conner & P. Norman (Eds.), *Predicting Health Behaviour: Research and Practice with Social Cognition Models* (pp. 81–126). Maidenhead: Open University Press. Retrieved from http://doc.utwente.nl/53445/

Notra, S., Siddiqi, M., Gharakheili, H. H., Sivaraman, V., & Boreli, R. (2014). An experimental study of security and privacy risks with emerging household appliances. In *2014 IEEE Conference on Communications and Network Security* (pp. 79–84). https://doi.org/10.1109/CNS.2014.6997469

Ohlhausen, M. K. (2014). Privacy Challenges and Opportunities: The Role of the Federal Trade Commission. *Journal of Public Policy & Marketing*, *33*(1), 4–9.

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health Services Research*, *34*(5 Pt 2), 1189–1208.

Peppet, S. R. (2014). Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent. *Texas Law Review*, *93*, 85.

Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big Data Privacy in the Internet of Things Era. *IT Professional*, *17*(3), 32–39. https://doi.org/10.1109/MITP.2015.34

Powers, T., Advincula, D., Austin, M. S., Graiko, S., & Snyder, J. (2012). Digital and Social Media In the Purchase Decision Process: A Special Report from the Advertising Research Foundation. *Journal of Advertising Research*, *52*(4), 479–489. https://doi.org/10.2501/JAR-52-4-479-489

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, *52*(3), 596–604. https://doi.org/10.1037/0022-3514.52.3.596

Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 1–17). USENIX Association. Retrieved from https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on* (pp. 163–167). IEEE. Retrieved from http://ieeexplore.ieee.org/abstract/document/7347956/

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2Nd Generation E-commerce: Privacy Preferences Versus Actual Behavior. In *Proceedings of the 3rd ACM Conference on Electronic Commerce* (pp. 38–47). New York, NY, USA: ACM. https://doi.org/10.1145/501158.501163

The Deloitte Consumer Review. (2016, July). Switch on to the connected home. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-16.pdf

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, *22*(2), 254–268. https://doi.org/10.1287/isre.1090.0260

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Vogelsang, I., & Compaine, B. M. (2000). *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy*. MIT Press.

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. https://doi.org/10.1016/j.bushor.2015.06.005

Woon, I., Tan, G.-W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 Proceedings*, 31.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Yang, Z., & Fang, X. (2004). Online service quality dimensions and their relationships with satisfaction: A content analysis of customer reviews of securities brokerage services. *International Journal of Service Industry Management*, *15*(3), 302–326. https://doi.org/10.1108/09564230410540953

Yang, Z., & Peterson, R. T. (2004). Customer perceived value, satisfaction, and loyalty: The role of switching costs. *Psychology and Marketing*, *21*(10), 799–822. https://doi.org/10.1002/mar.20030

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Z, S. (2005, June). Content analysis: Introduction. Retrieved May 21, 2017, from http://psc.dss.ucdavis.edu/sommerb/sommerdemo/content/intro.htm

Zorzi, M., Gluhak, A., Lange, S., & Bassi, A. (2010). From today's INTRAnet of things to a future INTERnet of things: a wireless- and mobility-related view. *IEEE Wireless Communications*, *17*(6), 44–51. https://doi.org/10.1109/MWC.2010.5675777

Appendix A- Interview Session Questionnaire

1. Do you prefer to shop from a physical store or an online store?
2. What measures do you take to learn about the product you're buying?
    a. How do you research the product? For example, reading reviews, comparing prices, and so on.
    b. How long does it take for you to buy the product? (in measure of hours or days)
    c. Why do you think it takes that much time? Or, what do you think is the benefit of being well informed of the product you are buying?
3. If you were to buy a smart home IoT device…….

    * Smart home IoT device image was handed out to explain the infrastructure of the system

    a. What information do you look for before you buy the device?
    b. How much do you know about privacy issues in smart home IoT devices?

    * The clippings from the HP report were handed out to help participants understand some privacy issues in smart home IoT devices

    http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

    http://go.saas.hpe.com/fod/internet-of-things

    c. What are your thoughts and impressions after reading the article
    d. Do you have any privacy preferences? What are your privacy preferences when you decide to buy a smart home IoT device?
    e. What are your preferences regarding collection of sensitive data and video or audio recording by home IoT devices?
    f. How many of those privacy preferences will you adopt to while buying the device? Or, how/why do those privacy preferences change during your purchase decision process?

g. Would you read news articles/blogs/forums to educate yourself on privacy issues in the smart home IoT device you plan on buying? What resources will you use to look for information on privacy issues?

h. If you had a privacy testing tool available online, do you think you would use it? Why or why not?

i. Will you incorporate these privacy protection measures into your purchase decision process? Why or why not?

j. Do you think these privacy protection measures will change your decision? Why or why not?

Appendix B- Interview Session Article Handouts

Smart Home IoT Devices

This image was handed out to participants during the study to explain the working of smart home IoT devices and their connection to mobile applications and cloud storage units.

Figure 4: Smart home IoT device connections

HP Study on IoT Security

Figures 5-9 represent clippings from two reports published by the HP company. These clippings were used during the interview session to highlight upon the existing privacy issues in home monitoring IoT systems.

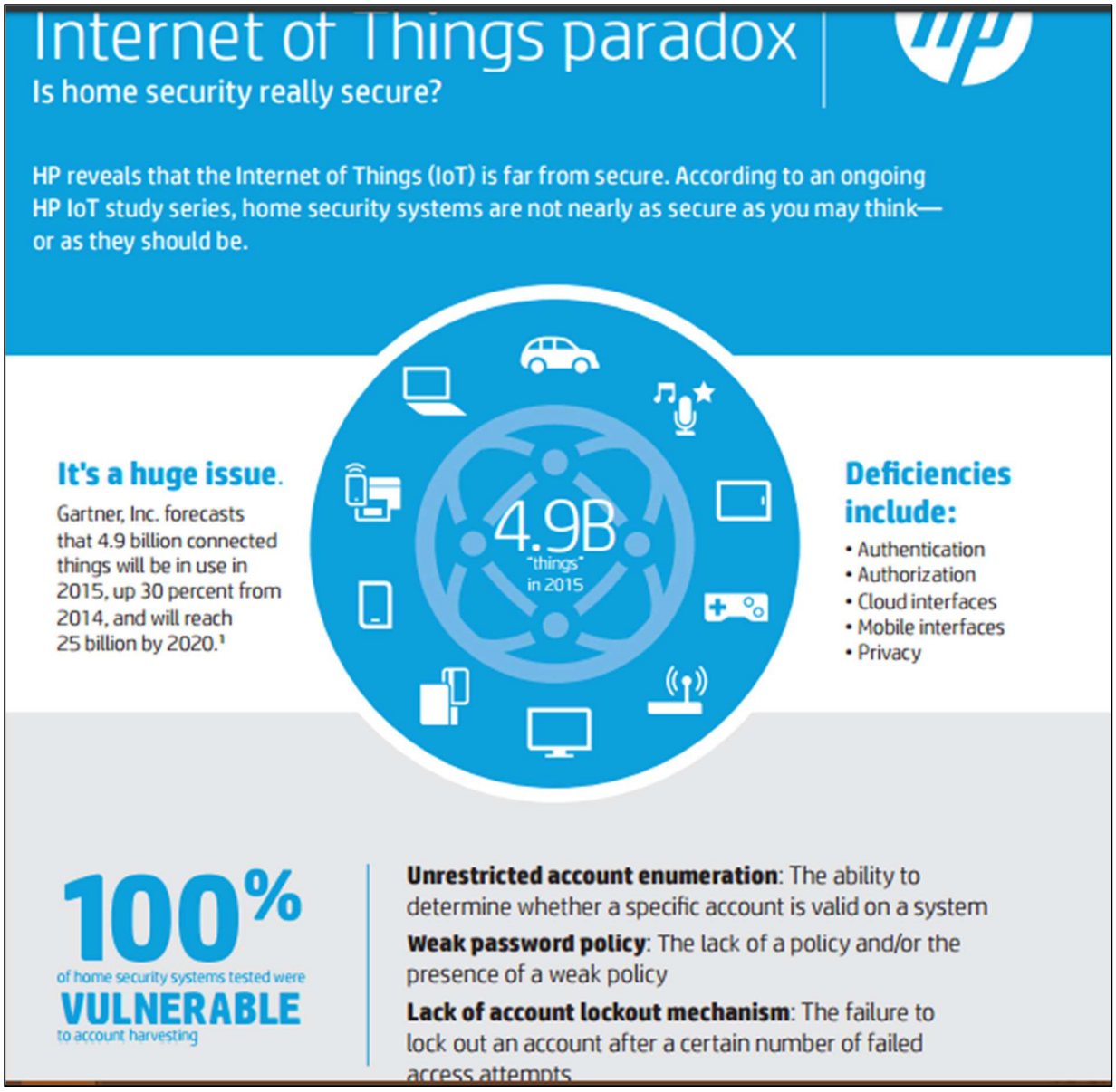

Figure 5: Title page of HP report- 'Home Security IoT Infographic'

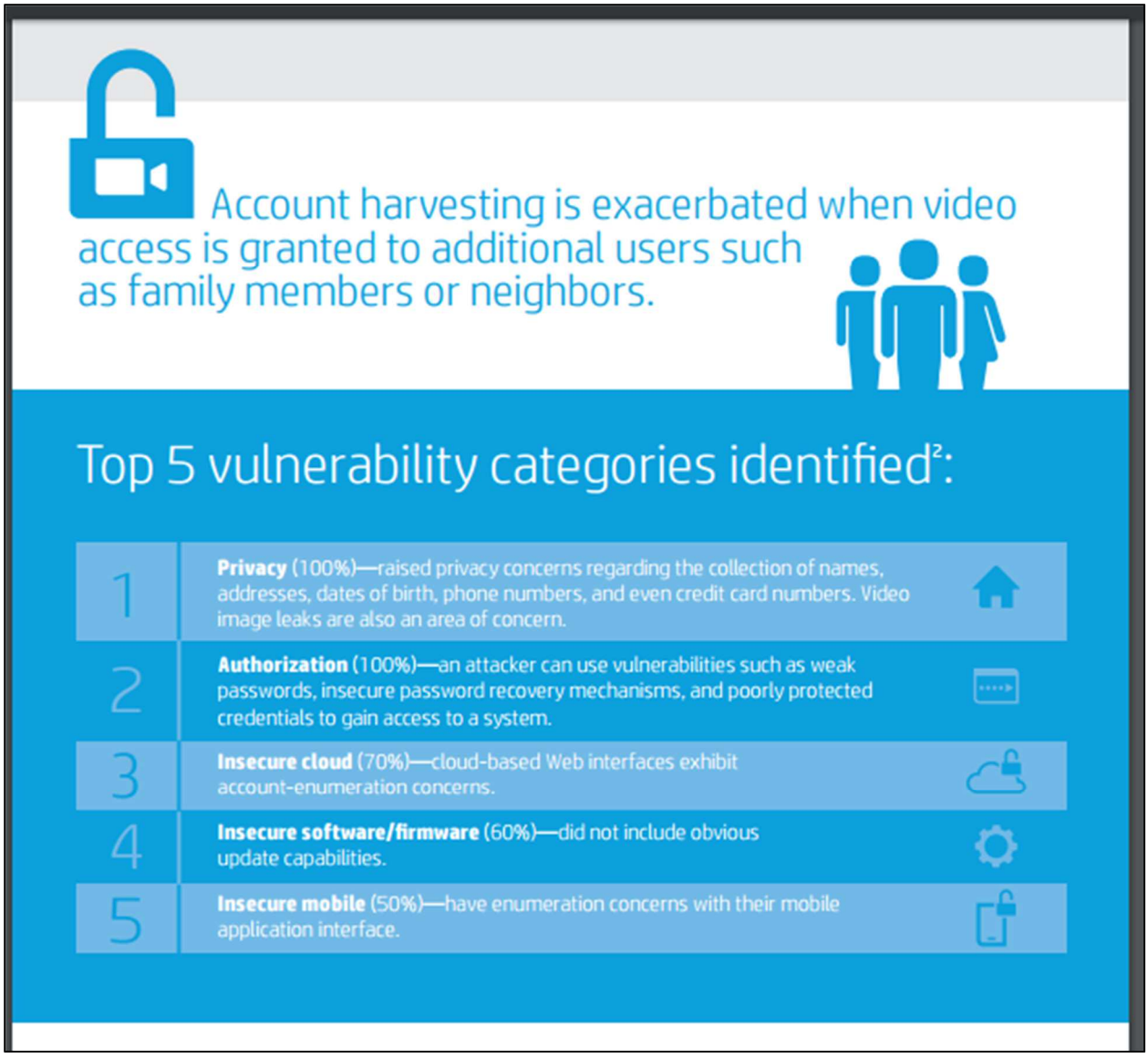

Figure 6: Clipping from 'Home Security IoT Infographic'

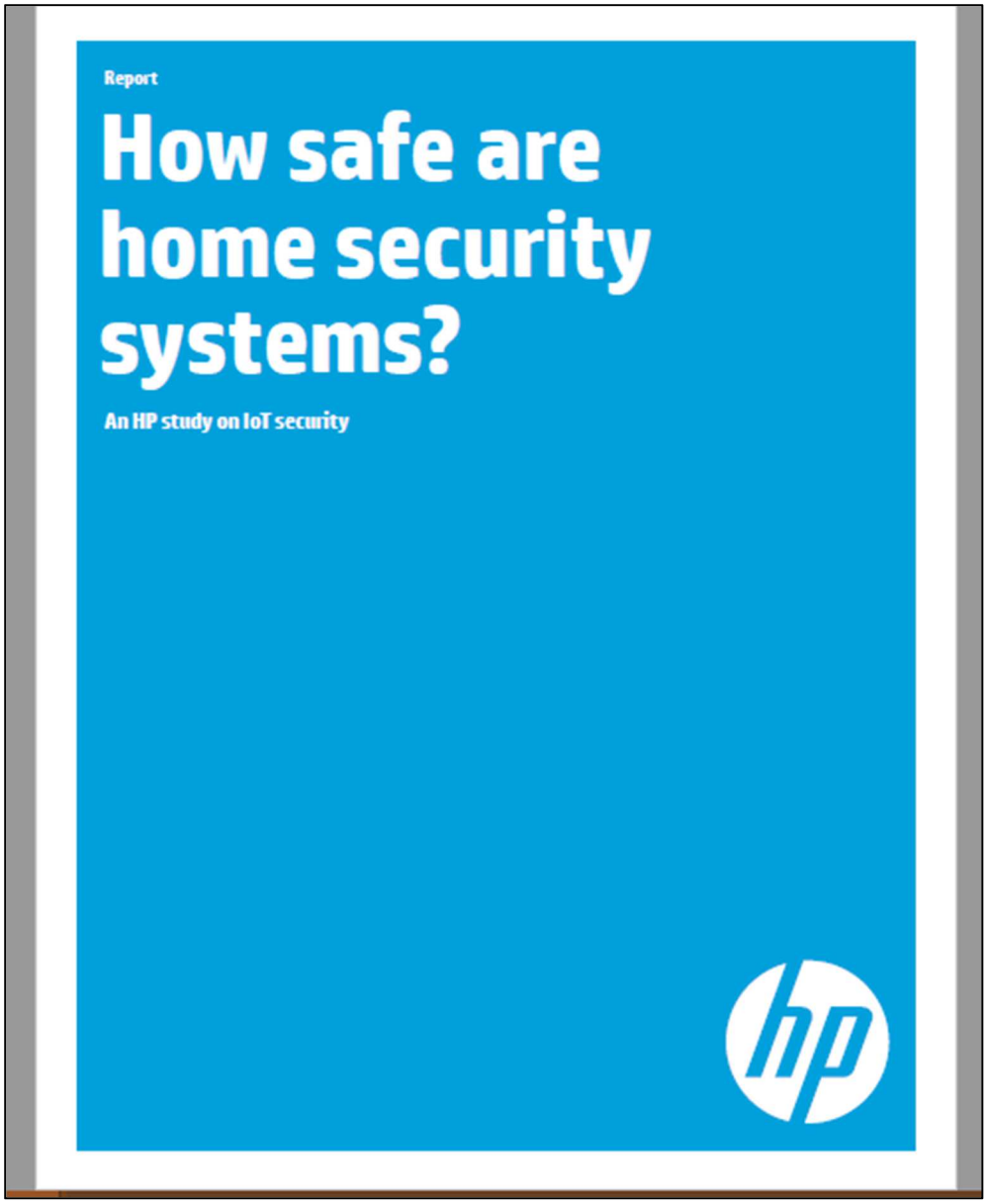

Figure 7: Title page of HP report- ‘IoT Home Security Systems’

Figure 8: Clipping from 'IoT Home Security Systems'

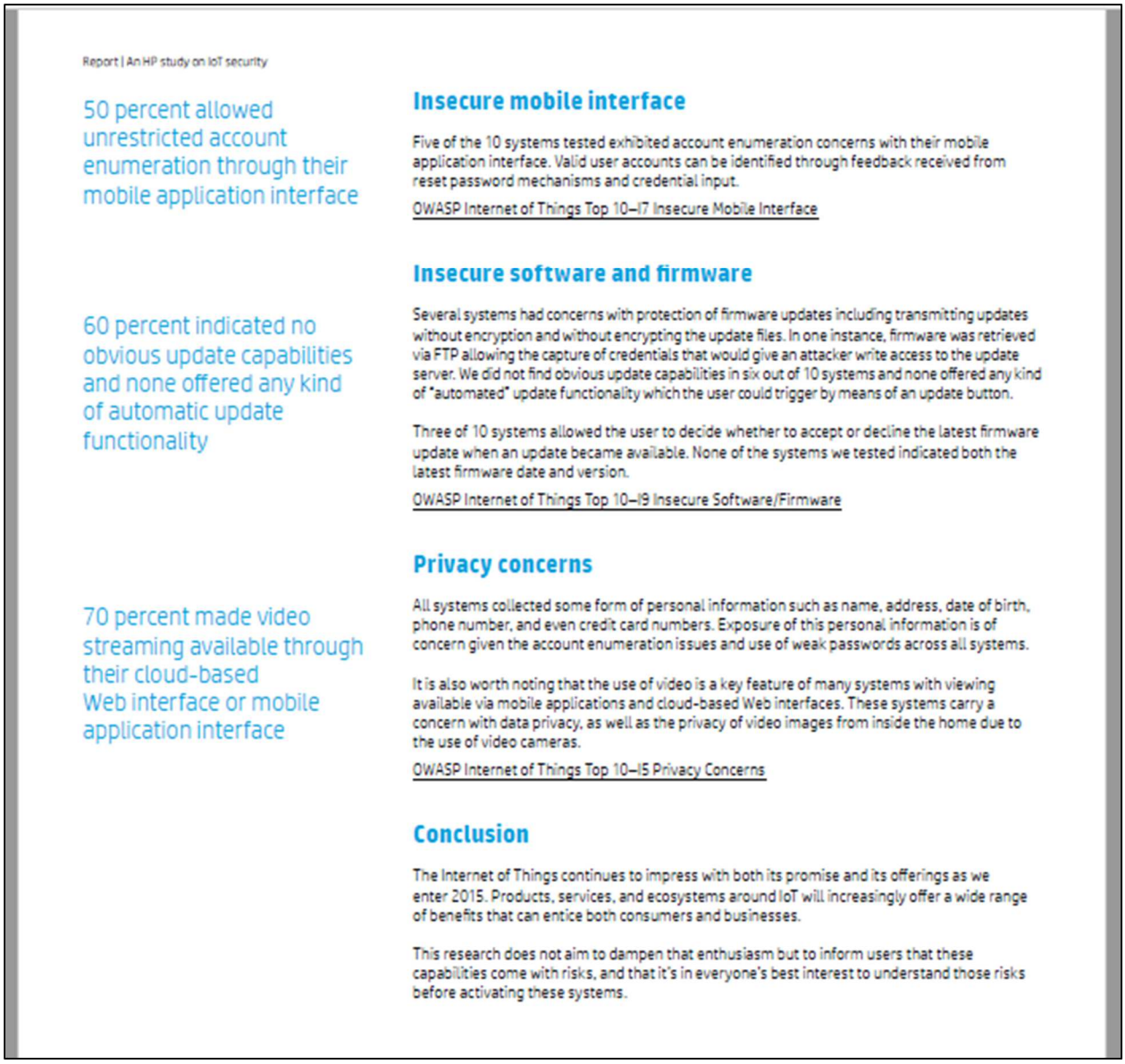

Figure 9: Clipping from 'IoT Home Security Systems'

Appendix C- Top 10 List of Smart Home IoT Devices

The following list of devices was selected from Amazon.com website's best sellers of the smart home category.

Table 5: List of top 10 smart home IoT devices

No.	Name of Device
1.	Alexa
2.	TCL Roku Smart LED TV (2015 Model)
3.	TP-Link Smart Plug
4.	Philips Hue White A19 Starter kit with two LED Light Bulbs and hub
5.	Nest Learning Thermostat, 3rd Generation
6.	Ecobee3 Thermostat with Sensor
7.	Arloo Security System
8.	Canary All-in-one Home Security device
9.	Nest Cam Indoor Security Camera
10.	Annova culinary Bluetooth/WiFii Precision cooker