2020

Smart Privacy for IoT: Privacy Embedded Design for Home Automation Systems

Love James

Smart Privacy for IoT: Privacy Embedded Design for Home Automation Systems

by

Love James

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Computing and Engineering
Nova Southeastern University

2020

We hereby certify that this dissertation, submitted by Love James conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Ling Wang, Ph.D.
Chairperson of Dissertation Committee

6/4/2020
Date

Junping Sun, Ph.D.
Dissertation Committee Member

6/4/2020
Date

Inkyoung Hur, Ph.D.
Dissertation Committee Member

6/4/2020
Date

Approved:

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

06/04/2020
Date

College of Computing and Engineering
Nova Southeastern University

2020

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Smart Privacy for IoT: Privacy Embedded Design for Home Automation Systems

by
Love James
June 2020

The emerging paradigm shift in technology to make everyday devices more intelligent than previously considered also known as internet of things (IoT) has further elevated the importance of privacy not only in theory but also in practice. The intrusive nature of these devices and in particular, the home automation system is also beginning to raise privacy concerns which might impact their usage either by deterring potential users from adopting the technology or discouraging existing users from the continued use of these home automation systems.

This study was an empirical and quantitative study that evaluates the impact of users' behavior when privacy is embedded into the design of home automation systems using a web-based survey. Prior to the main study, a Delphi study and a pilot study were conducted. A 5-point Likert scale was used for the survey items which was distributed, and 330 responses were received. A pre-analysis data screening was conducted prior to the data analysis and the Partial Least Square Structural Equation Modelling (PLS-SEM) was used to analyze the collected data, while the PROCESS macro for SPSS was used to evaluate the mediation effects of the model associated with the study.

The findings from this research show the mediating effects of privacy concern on the relationship between privacy embedded design and home automation usage as well as the relationship between privacy self-efficacy and home automation usage. The study also shows that both privacy concern and home automation usage predict the two antecedents for the study. While the finding shows that the mediating effects of privacy concern on the relationship between privacy self-efficacy and home automation usage is a full mediation, the mediating effects of privacy concerns on the relationship between privacy embedded design and home automation usage shows a complementary mediating effects. The findings in this study contributes to the information systems security and privacy body of knowledge by revealing the capacity of privacy concern to predict the behavior of users of home automation usage.

In Loving memory of my Father

James Oriloye

Acknowledgements

My profound appreciation goes to God Almighty for making this doctoral degree a reality. I am also incredibly grateful to my dissertation committee chair Dr. Ling Wang for her patience, guidance, and dedication through out the dissertation process. Her tireless effort and extensive knowledge have enabled me to reach all the milestone set for the completion of this dissertation. You are awesome!

My gratitude also goes to my amazing committee members, Dr Junping Sun, and Dr Inkyoung Hur; this would not have been a reality without your dedicated support and expertise. Your attention to details, constructive feedback and recommendations were tremendously phenomenal. I am highly grateful for all your help.

To my mother Mariam Oriloye, you inspired me more than you will ever know. Thank you for believing in me and for your continuous prayers, support, inspiration, as well as the constant encouragement you provided throughout this academic pursuit. Lots of love mama, you are simply the best!

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

The internet of things (IoT) is a technology paradigm whereby ‘everything’ is interconnected; however, these devices’ interconnectedness whether online or offline creates serious security and privacy concerns.

This concept of IoT, which interconnects and exposes almost everything through the internet was first proposed in the late 90s as sensor networks (Kong, 2008) and was predicted at the time to be among the ten technologies that would change people’s life in the future (Iborra, Álvarez, Losilla, Vicente-Chicote, & Sánchez, 2007). With this prediction gradually getting fulfilled, it is no longer news that devices including home automation devices can now interact with the environment they reside as well as with each other through internet connections and also have the capability of exchanging data with other applications.

Activities previously considered a science fiction scene where refrigerators can communicate with cars to drive their owners to grocery from work rather than home when it receives signals of low milk level from the fridge as well as washing machines messaging users when laundry needs to be done, are now a scary reality. While the intelligence of these networked smart devices in particular the home automation systems can be commended, their attendant convenience further breeds security and privacy

concerns that can deter potential users from embracing the benefits associated with their usage.

A prior research has revealed that numerous security and privacy challenges faced with the use of IoT devices include authentication and authorization of entities introduced to the system (Abomhara, & Køien, 2014). While another research emphasizes the challenges of information privacy in IoT technologies because the devices are not designed in ways that offers privacy protection for the consumers of such technologies. (Fenz, Heurix, Neubauer, & Zimmermann, 2015).

In 2014, the Federal Trade Commission of the USA settled a complaint against electronic manufacturer whose security vulnerabilities associated with the use of their IoT products exposed the private lives of users for public viewing on the internet (FTC, 2014). The experience of those involved in this security lapse can be described using the caption of an old TV show "Smile. You're on Candid Camera" however, if any of the words in this caption is to be taken seriously, the hundreds of consumers of these so-called security cameras whose private lives were watched online obviously would have nothing to smile about.

In a similar development, the Norway's Consumer Council logged a complaint with the Norway's data protection authority about the privacy policies of four fitness wristband companies on how their IoT products had broken local laws governing the handling of consumer data (Kaldestad, 2016). This was not limited to the wristband as some Norwegian toy companies were also found guilty of the same security and privacy violations (Myrstad, 2016).

The privacy challenges associated with IoT devices and especially the home automation system is compounded by the ubiquitous nature of the technology adopted in the design of most home automation systems such that users are either unaware of the privacy settings within the device or those settings are embedded in a way that is out of reach to the users (Mao, Senel, Keshavarzian, & Tozlu, 2012). Hence users mostly have no control over the invasion of their privacy by these devices and as such are unable to protect themselves against such invasion. The onus is therefore on the manufacturers to design the system in ways that would offer adequate privacy protection to users by default through the embedding of privacy into the design of the system.

Previous studies on privacy concerns with system usage have mostly concentrated on users' behaviour with respect to online transaction and information disclosure (Dinev & Hart, 2005; Dinev & Hart, 2006; Li, 2014; Dinev, Smith, & Xu, 2011), however very few studies have empirically examined the privacy concern associated with the use of home automation systems. In particular empirical studies to evaluate users' behaviour to home automation usage when privacy is embedded into the design of the home automation systems as an antecedent to privacy concern while also considering other antecedent factor of the privacy self-efficacy is yet to be found. This paper thus empirically evaluates the impact of privacy embedded design on users' behavior to the use of home automation systems.

Problem Statement

Several research studies have been carried out to help proffer security solutions to address the vulnerabilities associated with IoT devices in order to make them more secured. The study by Weber (2010) focused on the legal perspective of privacy

challenges of IoT and proposed a solution that involves the development of adequate framework based on the underlying technology of IoT to guide their deployment. While another study also suggested a holistic framework to address the challenges of privacy concern and privacy risks associated with the complexity of industrial IoT (Sadeghi, Wachsmann, & Waidner, 2015). Additional study equally expresses concerns about privacy issues that will be attendant to the use of IoT and suggested the development of new methodology to address these security and privacy challenges (Abomhara, & Køien, 2014). Some researchers have also identified privacy concerns as a very important factor impacting the large-scale applications of IoT and proposed a solution of adopting encryption mechanisms for IoT devices to protect the data they process (Bao, Huang, Sun, Yang, & Wang, 2014).

Arias, Buentello, Hernandez, and Jin, (2014) pointed out that it is relatively easy to compromise the home automation system and potentially make them become a botnet and can also be used to introduce rogue devices by attackers to subsequently compromise the network to which the devices are connected. In addition, when a particular home automation system is compromised, it can be used to search for exploitable vulnerabilities in other home automation devices on the network thereby providing a 'backdoor' to the users' network without them knowing (Hernandez et al., 2014). All these and many other security and privacy concern associated with the home automation systems lend credence to the fact that these devices can continue to spy on not only the activities of the inhabitants of the home but also their online activities without them knowing let alone safeguarding against it (Hernandez et al., 2014).

Home automation system by nature have less security and privacy features. The size of the devices makes it difficult for the in-built sensors and actuators they require to function to be easily updated or patched for them to be secured (Tozlu, et al., 2012). This challenge further creates the concern of how the data they collect from the environment they operate is being handled in terms of storage and transmission to protect users' privacy (Peppet, 2014). Despite the various researches conducted on the privacy challenges of home automation systems, there is still a dearth of research on how incorporating privacy into their design will impact the behaviours of users of these devices. The need for such studies has hence become highly relevant as the vulnerabilities from these devices have been associated with major privacy incidents with legal implications (Peppet, 2014).

As stated in the foregoing, most of the prior studies performed on users' behavior and privacy concern have been mostly with regards to online transactions with very few on the privacy concern and user behavior for home automation systems. They have also mainly focused on how users react to providing private information on a website during transaction leaving the gap that currently exists for specific studies in situation where the users are not presented with any option of consent to the invasion of their privacy. Given that the use of home automation systems presents several challenges to users, this research is an attempt to fill this gap.

Given that not much has been published in literature with regards to research using privacy embedded design as antecedents to privacy concern or as an independent variable to home automation usage, this research thus differs from the aforementioned. It also used theoretical and empirical approaches to investigate how embedding privacy into

the design of home automation systems will impact users' behavior to its adoption for use.

Dissertation Goal

The goal of this study is to assess the user behavior of home automation system when privacy is embedded into their design, a concept that has been termed in this study as privacy embedded design in order to address the prevailing privacy concern associated with the use of home automation systems. The privacy calculus theory (PCT) by Dinev and Hart (2005) was deployed in this research study. The study also adopted constructs that have been adapted from the PCT to investigate the privacy concerns that users have for the use of home automation systems and the effect of embedding privacy into the design of these systems on users' behavior.

Using the PCT and incorporating the concept of privacy paradox as well as the bounded rationality theory, the research study examined the consequent outcome when the antecedents to privacy concern are incorporated into the PCT to evaluate the outcome in terms of users' behavior. This study provides contribution to the information systems (IS) security research and practice through the use of theoretical and empirical perspective to investigate and propose the privacy embedded design as an antecedent factor to privacy concern based on the constructs from the antecedents →privacy concerns → outcome (APCO) model as proposed by Smith, Dinev and Xu (2011). The research also reveals how the privacy embedded design for home automation systems influence users' behavior through their willingness (or otherwise) to adopt and use these devices.

Research Questions

The research study seeks to provide answers to the following research questions based on the constructs in the research model:

1. To what extents will privacy embedded design interact with privacy concern to impact home automation usage?
2. To what extent will privacy self-efficacy interact with privacy concern to influence home automation usage?
3. How will privacy concern influences home automation systems usage?

Relevance and Significance

Despite the fact that the PCT is a useful theory in evaluating the factors that are antecedents to users' behavior (Dinev & Hart, 2006), the belief that calculus strengthens the factors that are antecedent to behavior may not be applicable in all situations especially with regards to the use of emerging technology such as the home automation systems; hence the need for this study.

The theoretical framework provided by theory of reasoned action (TRA) as proposed by Ajzen and Fishbein (1980) as well as the theory of planned behavior (TPB) (Ajzen, 1988) is the foundation for PCT which has provided a useful model for evaluating the behavioral outcome when antecedent factors to privacy concern are incorporated. The PCT model can therefore help to evaluate how individuals use the emerging technology such as the home automation systems by providing an insight to the extent in which users react to the norms associated with privacy concern when privacy is embedded into the device, which is consistent with the TRA (Ajzen & Fishbein, 1980).

Previous studies on privacy concern have been associated mostly with the link between privacy concern and outcomes with very few paying attention to factors that are antecedents to privacy concerns contained in the APCO model (Smith et. al, 2011). According to Smith et. al., (2011), passivist empirical studies that focus on antecedents to privacy concern to obtain outcomes would add great value to the privacy literature in IS research studies. Their study also reveals that theoretical and empirical studies on the link between the antecedent constructs that make up the APCO model are mostly lacking in IS literatures due to heavy reliance by researchers on TRA and the assumption that stated intentions will equate actual behavior based on the privacy paradox.

Given the above and considering the fact that not many have been provided in literature with regards to the emergent behavior of users with respect to the adoption and willingness to use the home automation systems if privacy is embedded into their design; it is therefore important to determine this antecedent factor using the APCO model. The study also evaluated how privacy concern mediates the relationship between this privacy embedded design and the privacy self-efficacy (both serving as antecedent factors) and the willingness to use the home automation systems which is the outcome to be considered in the model. The result of this research study therefore helps to shed more light on the prevailing argument on the privacy paradox of the contradiction between users' preference and their behavior with regards to privacy concern (Ackerman, Cranor, & Reagle, 1999). The other relevant construct as an antecedent factor (i.e. privacy self-efficacy) was also considered in this study.

This study hopefully provides some significant contributions to the IS literature. Firstly, it is hoped to be among the few studies on privacy that focuses on factors that are

antecedent to privacy concern, a construct that serves as the mediating variable in this study. Secondly, as other prior literatures on privacy concern have not dwelt so much on actual behavior as outcome in the PCT model, this study combines the uniqueness of focusing on users' actual behavior in addition to the antecedent factors to privacy concern. It is also hoped that the potential contributions that results from the empirical evidence uncovered during this study is helpful to fill the existing gap within the pool of IS literature on privacy concern. Additionally, the study also offers practical implications regarding the design of IS artifacts to enable manufacturers of home automation systems design these systems with the users in mind.

Barriers and Issues

The unpredictable nature of human behavior made it difficult to adequately measure the outcome of this research study. Given the fact that home automation system is an emerging technology which means that not many people have adopted its use. It should however be noted that users of other everyday home devices like the thermostat, the smart television and fridges, security cameras were categorised as home automation systems users in this study and were included as part of the survey participants. In addition, the anticipated challenges of obtaining the right sample size of population to participate in the survey was not encountered as an appropriate sample size that is proven to be sufficient for the analyses of this nature was obtained.

Assumptions

Researchers often refer to assumption as what is accepted to be true in a research without concrete proof (Larsen & Lee, 2009), hence for this study, in addition to building on the assumption of the PCT that a consequentialist trade-off of costs and benefits is

salient in determining an individual's behavioral reactions (Dinev & Hart, 2005), it also assumes privacy concern to be the measurable proxy for privacy. Other assumptions include: 1) the response of participants to the survey questions were sincere; 2) participants understands the meaning of home automation systems.

Limitations

One of the limitations associated with web-based survey (online google survey) which was adopted for this study is: self-selection bias (Parker & Rea, 2014) as only participants conversant with the subject matter may complete the survey correctly. In particular is with regards to the home automation usage construct as the understanding of the willingness of respondents to adopt or use the home automation systems is probably not a representation of the actual use behavior by these respondents.

Another limitation of the study is that the collected data which was sourced from the various cities in the Eastern and Western Canada may not be varied enough to represent the diverse users of the home automation systems as the results cannot be generalized.

Delimitations

As a delimitation to the self-selection bias, the survey questions were made very simple and easy to complete by the respondents. Efforts were also made to ensure that data collected are gathered from users as well as potential users of home automation systems. The results of the study have not been generalized and recommendations were provided for further study in other jurisdictions within and outside of Canada.

Summary

The need for a more secured design of home automation system that will ensure the privacy protection for users cannot be overemphasized. However, most of the previous researchers' focus for a secured home automation system had been majorly on the technical aspect of the study with most studies providing the suggestions to the technical features that would enhance the security of these devices. Based on positivists' theories that incorporate the PCT, privacy paradox and the bounded rationality theories, this study seeks to empirically evaluate what the outcome of users' behavior would be if privacy is embedded into the design feature of the home automation system.

This introductory chapter provides a background to the research with the problem statement identifying what the specific problem within the IS field to be investigated as well as why it constitutes a problem and its implications. The goal of the study was also elaborated upon with the identification of appropriate research questions indicating the focus of the research. The relevance and significance of the study was presented to further buttress on the importance of investigating the identified problem. The assumptions made in the study were presented while the potential limitations and delimitations to the research were also highlighted.

Chapter 2

Review of the Literature

Introduction

It has been estimated that by the end of year 2020, there will be over 50 billion network connected devices majority of which will be IoT (Hernandez et al., 2014) and as the intelligence of technology services continue to develop exponentially; the intrusive nature of this capability has continued to generate increased privacy concerns by researchers (Abomhara & Køien, 2014; Bao, Huang, Sun, Yang & Wang, 2014; Sadeghi, Wachsmann, & Waidner, 2015). The interconnectivity of networked devices has also created a breeding ground for attackers to exploit the associated limitations and weaknesses of these devices because an environment with billions of devices often lead to the potential abuse of all exposed flaws and weaknesses (Carskadden & Covington, 2013). Several studies have shown that, despite the advantages and convenience offered by IoT, there had been numerous security and privacy concerns associated with their use in particular with the home automation system devices (Abdulrahman, et.al., 2016; Bergmann & Lin, 2016; Hjorth & Torbensen, 2012; Sadeghi, Wachsmann, & Waidner, 2015).

According to a market study by Growth from Knowledge (GFK) a fourth largest market research organisation in the world (GFK, 2016), home automation systems is currently the most sought after among the IoT devices with half of the over 1000 adults

aged sixteen and over interviewed in selected countries internationally believing that home automation system (also known as smart home technology) will make an impact on their lives in the next few years. The literature review for this research study is focused on synthesizing other related studies by examining how theories and methodologies of previous studies is related and to identify the existing gaps. The chapter is aimed at providing insight into the approach and methodologies adopted by previous studies with similar focus.

Theory Development

Previous research studies have shown that individuals make decisions on issues relating to privacy concern without having a full knowledge of the consequences of such decisions. In addition, the idea of choosing ease and convenience benefitted from the use of certain technologies over the associated risks to their privacy invasion have not been fully explored in the information system research. This study therefore seeks to close this existing gap through the use of theoretical and empirical approaches to investigate the impact of embedding privacy into the design of home automation system on users' behavior. This users' behavior to the adoption of the home automation system is referred to as home automation usage.

The conceptual model for this research used the PCT to evaluate what users' behavior to the adoption and use of home automation systems would be when privacy is embedded into the design of these devices. Based upon the assumption that personal information can be likened to consumer products, scholars have used the cost-benefit-analysis method referred to as *privacy calculus* to enhance their research on personal information disclosure (Chellappa & Sin, 2005; Dinev & Hart, 2006). However, these

studies have been mostly based on private information disclosure with regards to ecommerce transactions and location-based services associated with mobile device usage (Abdullat, Babb, Furner, Keith & Lowry, 2016; Agarwal, Kim, Malhotra, 2004; Chellappa & Sin, 2005; Dinev & Hart, 2006; Dinev, Hart, & Smith, 2011; Van Dyke, Midha, & Nemati, 2007; Xu, Li, 2014).

The privacy concerns associated with online transactions also known as ecommerce whereby personal information are often collected, analyzed and transmitted among multiple platforms have necessitated the need for many researchers to create a rich stream of study that provide several factors why users disclose personal information online despite the attendant privacy concerns. Further, the various prior studies using the PCT have mostly measured users' privacy concerns in general terms (Dinev & Hart, 2006; Li, 2014; Xu, 2011) such that online vendors only need to convince users of the benefit of information disclosure in order to make them disclose their personal information. As suggested by Valacich and Wilson (2012), this situation-specific privacy calculus affects users' calculations of risks and benefits and have been mostly used in these studies to explain the privacy paradox phenomenon in relation to privacy concern and user behavior. Furthermore, for the most part, these prior studies have mostly used privacy concerns as the main independent variable that determines users' behavior.

Moreover, Chellappa and Sin (2005), in their study consider privacy concern as antecedent construct to study the consumers' concern for privacy in using personalization services in online transactions. Other researchers have also followed the notion of privacy concerns and adopted similar methods of privacy concerns as the independent variable to user behavior whereby users are presented with benefits in order to disclose personal

information without considering the associated concern to privacy (Xu, 2011). The study by Ellis, Lowry, Posey and Roberts, (2010), introduces privacy concern as a construct that increases the belief about specific risks to online personal information disclosure while Cao, Everard and Lowry (2011) also adopted a similar approach to the privacy concern construct.

The use of PCT model in the study by Keith et. al., (2016) adopted privacy concerns construct as a control variable to evaluate a location-based service without hypothesizing its relationship with other constructs. Additionally, Li (2013) introduces privacy concern as a mediator in their research to evaluate users' disposition to online privacy beliefs to personal information disclosure during online transactions. Although the research by Li (2013) to introduce privacy concerns as a mediator to antecedent factors of a multi-level model follows the recommendation by Xu et.al., (2011), which calls for more studies that evaluate the antecedent to privacy concern, Li's research is only limited to online transactions and the outcome for the study is based on behavioral intention and not on actual outcome.

The privacy concern construct in this research also follows the recommendation by Xu et. al., (2011) as previously stated, to add to the few existing studies that focus on other factors that are antecedent to privacy concern to users' behavior. Additionally, with the wide use of privacy concern as a multi-dimensional construct, it is adopted in this study as a situation-specific privacy concern (Pavlou et. al., 2007).

Further, this study also considers the factors that influence individual's behavior as found in the privacy paradox (Brown, 2001) and the bounded rationality theory (Simon, 1972). Rationality referred to the style of behaviour appropriate for achieving a

set goal under a certain condition (Simon, 1972). Models that have considered the theory of bounded rationality have been with regards to situations in which the individuals involved in achieving a task or making a decision, have incomplete information about the consequences associated with the situation involved in such decision-making process (Simon, 1972). Another research model involves the use of bounded rationality for situations that assume individuals to be able to make calculations for specific actions among possible alternative actions that is made available to them (Simon, 1972).

While both model assumptions for bounded rationality are individually applicable in this research study, the focus was to blend the two model for application in this study. According to Selten (1999), analytical approach to a decision task is based on the relationship between choice and outcome and the use of available information for the calculation of a solution. However, when a decision task is taken without enough information to make the required calculations about the potential consequences on the outcome of such a decision; it can result in unexpected behavior by the individual undertaking the task. This phenomenon can lead to privacy paradox which was also considered in this study.

The decision making process on issues related to privacy concern is influenced by factors part of which are incomplete information and systematic psychological is influenced by factors part of which are incomplete information and systematic psychological deviations from rationality (Acquisti, 2005); as such the outcome of such decisions can be influenced by these factors and consequently the behavioral outcome. Consequent upon this, researchers have studied and provided examples of how privacy behavior and attitudes have differed (Valacich & Wilson, 2012). The situation whereby

users report concerns for privacy, but such concerns do not correlate well with disclosure of their personal information during online transactions have been widely researched (Valacich & Wilson, 2012). This paradox to privacy has been explained with the notion that situational factors often override privacy concern especially with regards to online transactions (Li, Sarathy, & Xu, 2011); research have also shown inconsistency and irrational behavior with regards to privacy concern by users of technology (Valacich & Wilson, 2012) leading to privacy paradox.

Drawing from the foregoing, the use of privacy calculus theory in this study assumes that users could make irrational decisions on privacy concerns with the use of home automation systems. This is because of the information asymmetry mostly associated with the home automation systems such that the required detailed information about the associated privacy concerns is not fully known to the users before the decision to use them is made. This study therefore uses the privacy embedded design and the privacy self-efficacy constructs as the antecedent to privacy concern while the outcome to be examined and evaluated is the home automation usage. The conceptual model is illustrated in Figure 1.

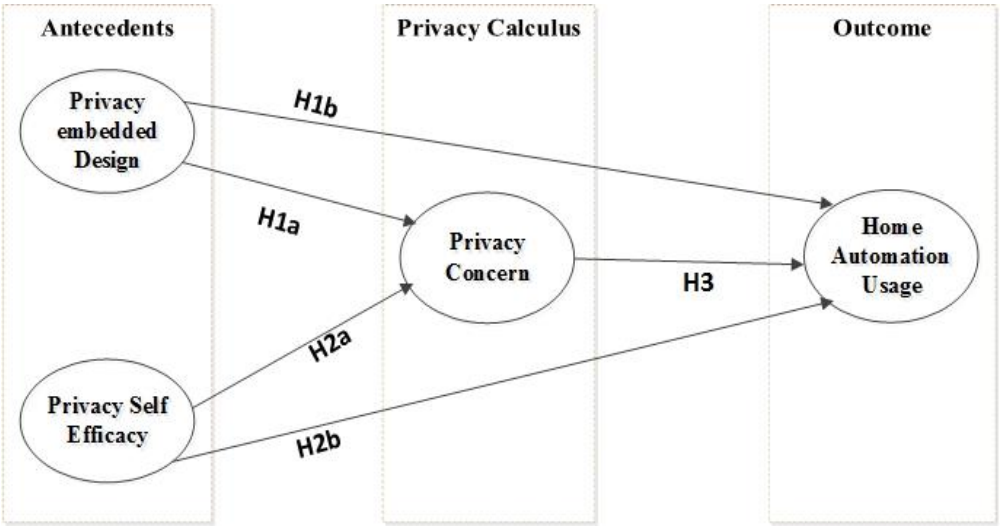


Figure 1. Research Model

Home automation usage has further increased the risk of concept drift which is brought about by extending the use of information for intentions other than that for which it was originally collected (Kalofonos & Shakhshir, 2007; Pishva, 2017). It is also beginning to raise the need not only for increased security, but also for the privacy protection of the users of these systems. Alam, Ali and Reaz, (2012) had pointed out in their work that the systems associated with home automation systems should be designed to be secured and safe for users in such a way that users' privacy would be protected. They also pointed out that home automation usage is generally driven by functionality and services, and as such users might be inadvertently unaware of the privacy risk associated with their usage. Therefore, there is the need for the designers of home automation systems to ensure that users' privacy is adequately protected by embedding protection features into the design of home automation system (Alam, Ali & Reaz, 2012).

Privacy embedded Design (PeD) refers to the concept of embedding privacy into the design of systems (Cavoukian, 2012). This is a borrowed concept from that of privacy enhanced technology (PET) (Hernandez et al., 2014). PET consists of systems of

technology measures that can be used to protect the privacy of users of such technology by preventing unnecessary transmission of the user information collected by the PETs (Borking & Raab, 2001). Some researchers have also referred to this concept as privacy-enhanced technology (Lou & Ren, 2008; Weber, 2010). This concept has continued to grow in its usage by various researchers with different focus to ensure the privacy protection of users of modern technology. Lou and Ren (2008) based their research on the development of privacy-enhanced security framework which is tailored for wireless mesh networks (WMNs) in order to address the security and privacy issues. Their research was aimed at proposing the use of strict user access control and sophisticated user privacy protection against both adversaries and other network entities (Lou & Ren, 2008).

A prior study by Boneh, Lynn, and Shacham, (2004) was also conducted to evaluate the signature scheme of systems as a protection mechanism for enhancing systems' security and privacy at their design stage of systems. A more recent research by Abdulrahman, et.al. (2016), also suggested that design and model implementation for home automation systems be simplified in order to deal with the problems of complexity and multiple incompatible standards found in the existing systems. Their study further proposed a design and model that is expected to ensure high level of security through the robust web services security protocol (Abdulrahman, et.al, 2016).

Additionally, the concept of privacy embedded design had been previously proposed to address the privacy concerns associated with how the breakdown of technological barriers has created the formation of a vast network of information and how

the growth of computer usage has resulted in the rise of personal surveillance (Cavoukian & Tapscott, 1996).

A number of researchers have adopted the use of privacy calculus in their studies to show the cost and benefits of the beliefs that influences users' behavior to privacy concerns and the consequent outcomes, although the studies were mostly focused on online transactions (Bies & Culnan, 2003; Stone & Stone, 1990). The PCT has also been adopted by other researchers whereby some have postulated the positive relationship between embedding privacy features into IT devices and their usage (Tan, Teo & Xu, 2005). However, drawing on the proposition by Dinev, Smith and Xu (2011) for the need of IS research studies that will examine outcomes that are a function of privacy-related independent variables as antecedents in the APCO model; the privacy embedded design therefore serves as one of the antecedents to privacy concern (PC) that influences consumers' willingness to home automation usage in this study and leads to the following hypothesis:

H1a: *Increase in privacy embedded Design will reduce the privacy concern for home automation usage.*

Moreover, other studies have been conducted to propose ways of forestalling privacy concerns. Some studies have shown the existence of a positive user behavior when privacy features are embedded into IT devices (Tan, Teo & Xu, 2005); while another study also reveals a positive user behavior in the presence of a privacy assurance with technology devices (Keith et. al., 2016). Extending this relationship to the APCO model for this study, it can be assumed that there will be a better assurance for users of

home automation systems when privacy is embedded into their design and thus positively impact their use behavior the following was therefore hypothesized:

H1b: *Increase in privacy embedded Design will cause an increase in home automation usage.*

Privacy self-efficacy (PSE) is defined in this study as the 'belief in one's ability to successfully perform a sophisticated privacy task'; as derived from the technology self-efficacy (TSE) concept (McDonald & Siegall, 1992). This construct is considered as a factor used by people to judge their capabilities to perform certain complex task (Bandura, 1986). Context-specific self-efficacy has been found to predict outcomes better and the role of context-specific self- efficacy has been found in several studies such as those on internet transaction (Vijayasarathy, 2004), compliance to security policy (Benbasat, Bulgurcu & Cavusoglu, 2010) as well as in security behaviors (Cho, 2010; Johnston & Warkentin, 2010). Bandura (1986) further pointed out that self-efficacy is a factor in determining an individual's actual behavior. In a similar manner, Abdullat, Babb, Furner, Keith and Lowry, (2015) also posited the effect of self-efficacy on behavioral change.

In this study, privacy self-efficacy will serve as the second antecedent to privacy concern to influence consumers' willingness to use the home automation systems and will assume the role of technology self-efficacy by integrating privacy self-efficacy as the belief in individuals' ability to protect privacy which has been shown to have a positive influence on use behavior (Youn, 2009).

Previous studies have addressed the linkages between antecedents and privacy concerns and these studies have found significant levels of association between privacy

concerns and outcomes (Belanger, Borena & Ejigu, 2013). Given that self-efficacy is the belief in one's ability to execute a particular task or behavior (Bandura, 1986), most especially with respect to one's confidence and ability to master new technology (Compeau & Riggings, 1995), a positive relationship have been found to exist between individuals with high self-efficacy and technology use behavior (Lai, 2008). Other IS researchers have also demonstrated how self-efficacy has led to the positive adoption of emerging technologies (Davis & Venkatesh, 1996; Morris, Speier & Venkatesh, 2002).

Drawing from the research by Van Dyke, Midha, and Nemati, (2007)on privacy empowerment, it can be said that most users of home automation system do not have the empowerment in the sense of the technical know-how that would enable them make a rational decision with respect to the use or otherwise of these devices given their associated privacy challenges. Empowerment have been mostly used in research studies from the management and organizational theory perspective in the context of employee empowerment and consumer empowerment to depict the granting of control to individuals (Van Dyke, Midha, & Nemati, 2007). The research by Thomas and Velthouse (1990) on the perspective of psychological empowerment, described '*competence*' as one of the four cognitions through which 'empowerment', is manifested. Their research interpreted *competence* as '*self-efficacy*' which is the ability to perform activities with skill (Thomas & Velthouse, 1990); this concept forms a major ingredient in control which is the basis of empowerment.

As privacy does not necessarily mean our information cannot be obtained, but rather the '*control'* we have over the information about ourselves that is exposed (Van Dyke, Midha, & Nemati, 2007), it can therefore be said that control is an important

concept in alleviating privacy concern and in turn have a positive impact on home automation usage. Further, the Federal Trade Commission's (FTC) Fair Information Practices (FTC, 2000) contains concepts about individual's empowerment to control their privacy. Given that the issue of individual control has been widely considered highly important in privacy management (Van Dyke, Midha, & Nemati, 2007), the privacy self-efficacy in this study is considered a surrogate for empowerment.

Additionally, the research by Baek (2014) has revealed that when individual have the required information for decision making, their behavior towards privacy concern is greatly impacted and this in turn creates a positive relationship with the outcome of individuals' behavior. In the same vein, Dinev, McConnell and Smith (2015), have also described how savvy users are able to take the necessary steps when using technology to inoculate themselves against the invasion of their privacy that could result from the manipulation of their personal information. Given the foregoing, the following hypotheses were therefore considered:

H2a: *Increase in privacy self-efficacy will reduce the privacy concern associated with home automation usage.*

H2b: *Increase in privacy self-efficacy will lead to an increase in home automation usage.*

Privacy has been used in a multi-dimensional concept (McCarthy, 1986) and some IS researchers have considered privacy to be the right of individuals to control the collection and use of information about themselves (Cahalane, Clarke, Daly, Fowler, Graham, Naughten & Robinson, 1991; Mason, 1986; O'Neil, 2001). Dinev and Hart (2005) have considered the notion of privacy concern as a multidimensional construct

where the concept has been researched widely as both a psychological construct (Goodwin, 1991) as well as social constructs (Laufer & Wolfe, 1977). The situation-specific privacy concern (Li, 2014) forms the basis of the privacy concern for this study. According to Li (2014), the situation-specific privacy concern deals with the uncertainties caused by the use of certain technology.

This study considers the privacy concerns created when networked and interconnected devices are connected to the internet with the potential of significantly extending, enriching and even shifting the relationship between people and the world in which they exist and operate (Leong, Koreshoff & Robertson, 2013). This is what is obtainable in technology the make up the home automation systems. Building on the assumption of the PCT (Dinev & Hart, 2006) that users can weigh the risks versus the benefits associated with their decision to use of home automation systems.

Additionally, a number of factors have been suggested as the cause of privacy concerns with the use of IoT and the design of the system; however, as pointed out by Hernandez et al., (2014), the IoTs' designers' lack of security knowledge appear to be the most common factor. One study on the security and privacy challenges in industrial IoT shows that the existing IoT devices are not sufficiently enhanced to fulfill the desired functional requirements and bear security and privacy risks at the same time (Sadeghi, Wachsmann, & Waidner, 2015). The proliferation of IoT devices have also been found to have led to a transparent society which will require a holistic cybersecurity framework to forestall the attendant privacy concerns (Sadeghi, Wachsmann, & Waidner, 2015).

Further, studies have shown the relationship between privacy concerns and individual behaviours and how these concerns constitute a negative impact (Li, Sarathy,

& Xu, 2011). Another research has also shown that no matter how 'sophisticated' individuals are, they may under certain conditions still become 'privacy' myopic but exhibit some privacy concerns in the use of technology (Acquisti & Grossklags, 2005). While the studies by some other researchers also prove the strong negative relationship between the level of individual's privacy concern and their behaviour to information disclosure (Ferrell, Nowak & Phelps, 2000; Miao & Yang, 2008). Accordingly, the following hypothesis was drawn from these studies:

H3: *Increase in privacy concern will reduce home automation usage.*

The home automation usage construct represents the outcome in the APCO model. This outcome is the users' behavior and a consequent factor of the model and the construct has been used in previous literatures mostly with regards to online transactions and information disclosure on websites. The outcome construct for this study was developed in line with the PCT following the research study by Li (2014).

Theoretical Foundation

Privacy Calculus Theory

Previous researchers have consistently tried to explain the predicting factors to individual behaviors with the most commonly used behavior related theories such as the theory of reasoned action (TRA) as proposed by Ajzen and Fishbein (1980) as well as the theory of planned behavior (Ajzen, 1988). The PCT helps to gain further understanding of the roles played by some antecedents to privacy concern play in users' behavior (Dinev & Hart, 2006). The PCT theory for this study was developed by Dinev and Hart (2005) following the model of the components of the TRA (Ajzen and Fishbein, 1980) and TPB (Ajzen 1988). As shown by information system literatures, the TRA and TPB

model have been used widely in information system research to investigate users' behavior by testing the component factors that are antecedents to user behaviors (Davis, 1989; Venkatesh et al., 2003; Yzer, 2017). TRA and TPB are mostly based on the fact that people behave reasonably although not rationally based on certain beliefs that they hold about such behavior; these theories also help establish the fact that individuals act on their intentions if they are not hindered by situational factors and they have the required skills (Yzer, 2017).

The PCT was adapted from the primary components of beliefs and behaviour associated with the TRA and TPB (Dinev & Hart, 2005) with the model been commonly used by researchers to evaluate users' behaviour associated with risks and benefit beliefs regarding privacy concerns. The PCT also employs a model that considers the antecedents to privacy concern and the consequent outcome (APCO) based on user behavior (Dinev & Hart, 2006). This was later expanded as the APCO Macro model to incorporate and test the contrary factors representing the elements of the PCT (Dinev, Smith & Xu, 2011) as shown in Figure 2.

PCT is used in this study because it provides an overall trade off of risk and benefit beliefs that lead to a user's behaviour in return for some anticipated benefits (Dinev & Hart, 2006). Thus, if a user considers that the benefits of using the home automation system outweighs the concerns to privacy, then it is expected that the user will adopt its use, otherwise they will not. According to Dinev and Hart (2005), the PCT considered the fact that there are other salient factors that contributes to users' behavior when personal privacy is involved. Their research show that individuals often consider

calculus or a decision process during internet transactions involving the disclosure of personal information.

The idea behind using the PCT and hence the APCO model is its potential to provide clues to users' behavior when they weigh the cost versus the benefits of using the home automation systems (Dinev & Hart, 2006). The study by Wakefield (2013), has shown that systems with appealing features could potentially influence the users' behavior to adopting its use. Thus, if users of home automation system find the devices appealing, they could still consider the costs versus benefits to using them despite the privacy concerns attributable to those devices.

However, studies have also shown this notion to be subjective based on the privacy paradox as noted by Acquisti (2004) whose work suggests that bounded rationality plays a major role on what constitutes users' decision on privacy concern because individuals have the tendency to discount the associated costs and benefits. Hence for the purpose of this study, additional components from the privacy paradox and the bounded rationality theory were integrated as factors to be considered while using the PCT model.

The assumption by researchers that private information can be likened to goods that can be traded when considering the cost-benefit calculation involved in the decision by individuals to disclose personal information has been termed the '*privacy calculus'* by Culnan and Armstrong (1999). This concept has been further expanded by IS researchers in the context of weighing the perceived risks and benefit involved in making a rational decision on the internet during on-line transaction (Dinev & Hart, 2006).

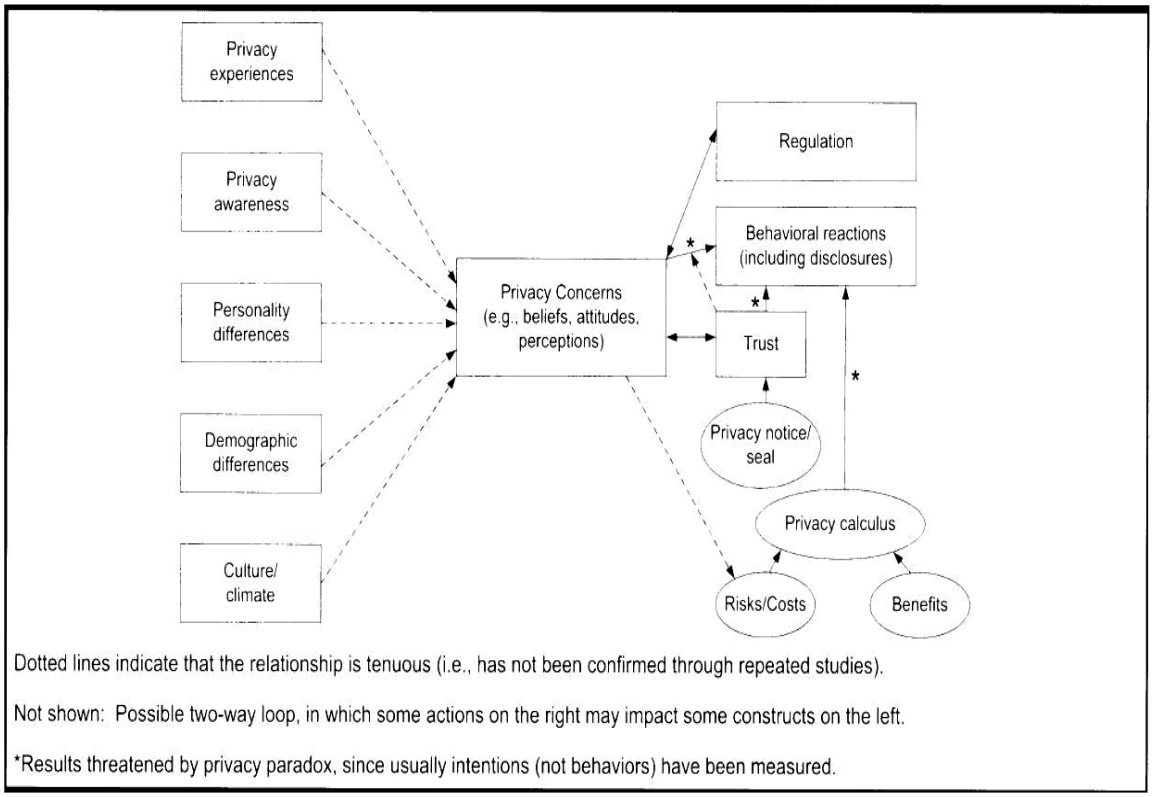


Figure 2. APCO Macro Model – Antecedents →Privacy Concerns → Outcome (Dinev, Smith and Xu, 2011).

Further, previous studies on users' responses to adopt the *privacy calculus* have shown that users are more willing to forego privacy concern if they found that the outcome of their action will be beneficial (Aloudat & Michael, 2011). Given that previous studies have only paid limited attention to factors that serve as antecedents to privacy concerns (Dinev & Hart, 2006; Dinev, Smith & Xu, 2011; Horne, Horne & Norberg, 2007; Yang & Miao, 2008); researchers are now indicating the need for additional study that will focus not only on the antecedents to privacy concerns but also on behavioral outcomes of such antecedents to shed more light on the privacy paradox (Dinev, Smith & Xu, 2011). Hence the need for additional research on users' behavior to privacy issues with focus on the home automation system using the PCT.

This study was conducted through an anonymous survey with the identified constructs based on the PCT. The constructs are privacy embedded design; privacy self-efficacy; privacy concern and home automation usage. Each of these constructs form the basis of the following review of related literatures.

Privacy Paradox

This is a situation whereby individuals expressed concerns about the invasion of their privacy but were still willing to provide their personal information during interactions with technology or the internet, mainly online transactions (Brown, 2001). The privacy paradox supports the claims by Acquisti (2004) that people sometimes acts irrationally when it comes to personal privacy. Acquisti also argues that individuals are affected by bounded rationality when making decisions related to privacy concern.

The main context of studies relating to the privacy paradox have been mainly with respect to social and transactional situations such as those concerned with e-commerce transactions and those with online networking media (Kokolakis, 2017). Additionally, research have shown that this paradox makes users seem inconsistent and unreasonable with regards to privacy concerns. However, for most users of technology, the ease and convenience derived from their usage and the desire to satisfy these needs far outweighs the associated privacy concerns (Lee et al., 2013). The study by Kokolakis (2017) also suggests that the PCT can be used to interpret privacy paradox given that PCT helps interpret how an individual uses calculus to evaluate the expected loss of privacy and the benefits to be derived from a particular behavior and this tradeoff often determine the expected outcome (Dinev & Hart, 2006; Xu et al., 2011). As such, incorporating the

concept of privacy paradox into the model for this study will provide some additions to the existing gaps in the IS research.

Many studies have been conducted using the PCT to support the privacy paradox concept and most have concluded that individuals will behave in a manner that help them achieve favorable outcomes. Certain factors have however been identified by scholars to be responsible for such behavior (Dinev, Smith & Xu, 2011). Some studies have shown that the anticipated reward by individuals could be one of the responsible factors (Caudill & Murphy 2000; D'Souza, & Phelps, 2009; Hann, Hui, Lee & Png, 2007); while another study pins the factor down to value personalization (Chellappa & Sin, 2005). A further study also reveals that the anticipated benefits associated with their behavior which the researcher refers to as the 'social adjustment benefit' could also be responsible for such behavior (Hui, Lu &Tan, 2004). All these desired outcomes have been proven by research scholars to override the privacy concerns that individuals have for the use of new technology even despite being aware of such concerns (Dinev, Smith & Xu, 2011).

Given that researchers have often used the privacy calculus theory in conjunction with the privacy paradox and bounded rationality, incorporating the concept of privacy paradox into this study will therefore provide some additions in the interpretation of the research results and thus attempt to close the existing gaps in the IS research. Additionally, despite the large volume of studies on privacy paradox, the studies had been mostly conducted using privacy paradox in isolation and its combination with other privacy theories are under-researched in the IS literature (Kokolakis, 2017). This study presents a unique combination of the PCT with privacy paradox in conjunction with the

bounded rationality theory to evaluate individuals' behavior within the technology environment.

Bounded Rationality Theory

Bounded rationality is the limitation faced by individual that prevent them from making a rational decision (Kokolakis, 2017). The PCT is based on the assumption that individuals make rational privacy decision by calculating the risks and benefits of their behavior, it has however been proven that most people lack the cognitive ability to calculate and determine when there is a privacy concern in technology usage (Kokolakis, 2017). This is especially true when they do not have the necessary information required to calculate the risks and benefits to make an informed decision. This has been further proven in cognitive psychology that they are unable to calculate the relevant parameters of privacy concern and that their decision is only made based on bounded rationality (Acquisti & Grossklags, 2005).

The expectations for users to behave in a rational manner is in line with the expectancy theory by Vroom (1964). This assumption in behavior is expected in order to maximize benefits and minimize costs and has underpinned most of the IS studies on involving privacy calculus. A study on the balance of benefit to the cost of personal information disclosure on the internet found that individuals will overlook the privacy concern associated with disclosing their personal information on the internet if they perceive the overall benefits of such disclosure outweighs the risks.

Despite the number of privacy studies that supports the assumption of the rational behavior of cost benefits by users of IS artifacts, especially with regards to internet disclosure, other studies have consistently challenged this assumption using the

behavioral economics principle (Acquisti 2004; Acquisti 2009; Acquisti &Grossklags 2003; Acquisti & Grossklags 2005; Acquisti & Grossklags 2007; Acquisti, Cranor, Egelman & Tsai, 2011). This behavioral economics perspective known as the privacy paradox is believed to be associated with a psychological distortion which discounts risks; it is also responsible for information asymmetry which results from users having limited information about the implication of their actions as well as the bounded rationality which is the inability to fully comprehend the probabilities of the costs and benefits of the privacy concerns associated with their intended actions (Acquisti & Grossklags 2003).

These limitations therefore explain why users make irrational decision when privacy concern is involved in the use of emerging technology such as the home automation system. Drawing from the asymmetric or limitation of information assumption, most users of home automation systems have little or no understanding of the design features of these devices and the level of associated security and privacy challenges their use could pose to them. As such, their decision to use these devices despite the associated privacy concern could be explained using bounded rationality. Tsai et. al., (2011) in their study explored these effects of information asymmetries and found that the reduction of information asymmetry through proper accessibility of privacy disclosure by online vendors causes more rational behavior in users.

The researchers in the aforementioned studies have by no means undermined the effects of rational decision-making but have alluded to the fact that users' behavior towards the use of emerging technology might not be wholly determined by rational thinking. Upon this backdrop, the research model in this study also introduces the privacy

self-efficacy as the second antecedent construct to the PCT model in order to examine the actual behavior as proposed by Smith, Dinev and Xu (2011). This is as a factor that was evaluated within the privacy calculus to proffer solution for addressing the privacy paradox. This evaluation was achieved by assessing users' calculation of the costs versus benefits associated with the home automation system usage while overriding the privacy concerns associated with such devices so as to achieve the benefits that comes with their usage.

Security and Privacy Challenges in Home Automation Systems

Privacy was initially considered a social concept whereby people adjusted their behaviour to accommodate the need for individual privacy. However, over the centuries it has acquired a quasi-legal whereby conversations between spouses or with doctors and lawyers were recognized as being privileged and sanctions set down in law against trespass but none of which referenced privacy protection (Ellis, et. al., 2010). A concise definition of privacy that has endured since first used by Warren and Brandeis (1890) is "the right to be let alone" – a definition that was borne as a result of technological advancement. At that time, Warren and Brandeis became concerned about how news reporting was becoming a wholesale enterprise regardless of how newsworthy the subjects were (Brandeis & Warren, 1890). This definition seems a perfect fit in today's age of technological invasion of privacy, especially through the use of IoT devices.

IoT as an intelligent object is able to collaborate, exchange and transmit information about its environment as well as react to events in their surroundings (Challal, Iera, Riahi, Natalizio & Mitton, 2014). The unique and pervasive ability of IoT uses various technologies in-built within them for data collection from different

component through sensors, RFID tags and readers thereby creating the risks of data privacy (Riahi, A., Natalizio, E., Challal, Y., Mitton, N., & Iera, A., 2014). Additionally, the large amount of human-centric data they generate and transmit between various networks can lead to the compromise of users' privacy through unauthorized information disclosure if adequate precaution is not taken (Riahi et. al., 2014).

The home automation system devices are considered as an example of IoT because they are typically embedded with sensors and actuators with the capability to extend network communications. This enables them to not only be able to monitor movements within the environment in which they are located, but also control features of other devices within their range (Delahoche, Durand, Loge, Marhic, Menga & Ricquebourg, 2006). The result of these capabilities by the home automation devices is that they can operate autonomously to manage the home without interaction with the users (Jacobsson et al. 2016).

As home automation systems are designed to improve home security, comfort that comes with convenience and the efficient use of energy, it has been estimated that about 90 million people around the world will use one form or another of the home automation system devices in the near future (Davidsson & Jacobsson, 2015). It has also been shown that households can maximise certain utility efficiency such as energy consumption through the use of these devices (Davidsson & Jacobsson, 2015). This capability has increased the rate at which the manufacturers of these devices invade users' privacy through the embedding of data-gathering sensors which could help obtain the necessary information required for the feedback required by users (Fensel, Kumar & Tomic, 2014).

The study by Lange, Kramp and Van Kranenburg, (2013), on smart home automation further reveals the security issues of communicating objects within the devices. Their study concluded that this might have been as a result of the resource-constrained nature of the components used in the development of home automation systems which prevent the implementation of standard security solutions for the devices. Other studies such as the one by Choi, Choi, Lee and Zappaterra (2014) also supports the fact that resource-constrained nature of home automation systems make them highly vulnerable to security attacks.

Security management concepts and principles are elements of solution deployment which not only define the basic parameters needed for a secure environment but also the goals and objectives that system designers and implementers must achieve to create a secure solution (Chapple, Gibson & Stewart 2018). Essential parts of the key concepts of security requirements are authentication, confidentiality, access control, and non-repudiation. This should be an essential focus for IoT and specifically for home automation systems as by nature they are enabled to foster constant transfer and data sharing among other devices and users in order to achieve a set objective (Coen-Porisini, Grieco, Sicari & Rizzardi, 2015). Given the sharing environment that the home automation systems create, these key requirements for security (i.e. authentication, authorization, access control and non-repudiation) are essential to ensure the security and privacy of the transmitted information. However, the lack of traditional computing capabilities by these devices necessitates the need for a tailored technique for them in order to achieve a secured communication amongst them (Sicari et. al, 2015).

Past Literatures

As the use of IoT and especially the home automation systems continue to grow, their security and privacy is equally becoming a serious concern both to the security and privacy practitioners, as well as the legal practitioners and regulatory authorities. Evidence of this can be observed at the various attempts that prior studies have made on how the design of home automation systems can be improved upon to ensure adequate protection for users.

The different aspect of research conducted in the past decades on the use of home automation system include the management of the interoperability and access controls of home automation systems (Hjorth & Torbensen, 2012). This was aimed at preventing the security issues arising from relying on third-party servers outside the home for the operation of these devices (Hjorth & Torbensen, 2012). Some studies have also proposed the design of a robust home automation system to address the problem of complexity and standards incompatibility that often leads to vulnerability issue in the devices (Abdulrahman, Isiwekpeni, Otuoze & Surajudeen-Bakinde, 2016; Bergmann & Lin, 2016). The home automation system is a device that is designed to use interconnected devices that deploys the 'smart' home technology in the home (Bergmann & Lin, 2016; Hernandez et al., 2014). A smart home was earlier defined as "the integration of different services within a home by using a common communication system" (Lutolf, 1992).

One of the key features of the home automation systems is location awareness (Alam, Ali & Reaz, 2012). However, the flow of information in these systems is generally unprotected across the multiple interconnected devices and over the internet through which it sometimes travels to report the gathered information (Alam, Ali & Reaz,

2012). Further, the ubiquitous nature of the design of home automation systems and the remote monitoring capabilities of its system components for better optimization of user experience has increased the security and privacy concerns associated with their usage (Alam, Ali & Reaz, 2012).

The need for a more secured design of home automation system that will ensure the privacy protection for users cannot be overemphasized (Babar, Prasad, Sen & Stango, 2011) proposed in their study, the embedding of security framework that provides built-in security for connected IoT devices. Their study was as a result of the investigation of network-based attacks on IoT systems which could put users at risk of security and privacy breaches. However, their work was only focused on enforcing security policies throughout the lifecycle of the development of the IoT.

Additionally, the report on system design issued by the Whitehouse offers a guide on addressing privacy safeguards in IoT devices during their design stage (Boldt, Carlsson & Jacobsson, 2016). This report is provided to ensure the security and privacy of the IoT devices at the development stage such that default settings of the devices are set to protect users' privacy and security at the time of purchase thereby ensuring the privacy protection for users with little or no technical knowledge of adjusting such settings. This also conforms to the publication by the National Technical Authority for information Assurance in the UK which published the properties required at the system design stage to ensure the security and privacy protection of users (Boldt, Carlsson & Jacobsson, 2016).

Identification of Gaps in Past Literature

Previous research on privacy concerns and technology use behavior have been mostly concentrated on how users can leverage the features within the technology (either devices or web interface) to protect the invasion of their privacy. Agarwal, Malhotra and Kim, (2004), in their research on the privacy concerns of internet users and their behavioral intention to release private information about themselves found that online consumers have control over the information they consider to be private. As such, the users may choose to or not to provide the information online due to privacy concerns (Agarwal, Malhotra & Kim, 2004).

Similarly, the study by Dinev and Hart (2006) using the PCT model to access users' behavior on ecommerce transactions provides an attempt at better understanding the balance between privacy risks beliefs and the users' intention to provide personal information during online transaction. The result of their study suggests that internet privacy concerns inhibit e-commerce transactions (Dinev & Hart, 2006). The conclusion of their research was that internet vendors should provide assurance of trust to their users by ensuring that their privacy is protected during online transactions (Dinev & Hart, 2006). Their research also reiterates the usefulness of the PCT for researchers as a model that is useful in studies relating to privacy concern.

In addition, Li (2014) also investigated the impacts of privacy concerns on online behavior during e-commerce transaction. The study found that the disposition to privacy concern is the only significant factor on users' intention to disclose information and transact on a website. It would however be noted that most of the previous studies on security and privacy challenges have been focused on users' behavior to the privacy of

personal information in electronic e-commerce (Dinev & Hart, 2006; Dinev, Smith & Xu, 2011; Horne, Horne & Norberg, 2007; Kokolakis, 2017; Miao & Yang, 2008; Valacich & Wilson, 2012); hence, this study focused on the privacy concern associated with users' behavior for home automation systems. The use of the APCO model in the research also helped to shed more light on the antecedent factors to privacy concern and their eventual outcome (Li, 2014).

Analysis of Research Methods Used

The various literatures reviewed to assess the use of PCT and APCO model for users' behaviour with regards to privacy concern have all adopted varying methodologies to perform their research study. These methods range from empirical study to experimental study as well as qualitative study of research methodologies. Majority of the empirical studies have been mostly focused on the privacy concerns with regards to internet usage and on-line transactions. For example, the study by Li (2014) to address the issue of privacy concern with a multi-level model for individual information privacy beliefs to understand the impacts of privacy beliefs on online behavior used a survey completed by 110 respondents. Xu et al. (2011) conducted a study on four different websites to examine the formation of individuals' privacy concern about specific websites also adopted the survey method with 823 respondents. In a similar vein, the studies by Dinev and Hart (2006) was also conducted using the survey method which included responses from 369 participants.

While most of the studies on privacy concern that uses the empirical methods had been focused majorly on e-commerce transactions, other studies on privacy concerns that adopted other research methodologies such as the experimental and qualitative studies

have their research focused on location based services for mobile devices as well as system design. Additionally, virtually all the reviewed literatures used the descriptive and inferential statistics methods. They also performed the construct convergent validity, discriminant validity, reliability and model fit. They also mostly adopted the structural equation modelling methods of analysis which incorporated tests such as Cronbach's alpha and goodness of fit tests.

From the foregoing it can be seen that, for the literatures that adopted the PCT for similar studies, only few focus their research on the antecedents to privacy concern and studies are yet to be found using the PCT that uses privacy embedded design and privacy self-efficacy as constructs antecedent to privacy concern. The few existing studies with similar focus have mostly dwell on users' behavior towards online transactions without addressing the factors antecedent to privacy concern. In addition, the dearth in IS literature for research studies that address users' behavior to the use of home automation systems when privacy is embedded into their design also provides a reason for this research study. A brief overview of the gap analysis from previous related research studies is presented in Table 1.

Table 1

Overview of related research for gap analysis

Researchers	**Research Focus**			**Findings on Privacy Issues**	**Methodology**
	Online[1]	Mobile (LBS[2])	System Design		
Culnan (1993)	X			The use of personal information by e-commerce vendors should adopt the fair information practice principle to	Empirical study

[1] E-Commerce transaction & behavior
[2] Location Based Services in mobile devices

Researchers	Research Focus			Findings on Privacy Issues	Methodology
	Online[1]	Mobile (LBS[2])	System Design		
				ensure users' privacy protection.	
Malhotra et al. (2004)	X			The internet users' information privacy concern model will be useful in analyzing the online privacy concern and reactions to various privacy threats on the internet.	Empirical study
Chellappa & Sin (2005)	X			Using trust building activities to protect the privacy of information of online transactions.	Empirical study
Dinev & Hart (2006)	X			Using the privacy calculus model to posit that privacy concerns inhibits e-commerce transactions.	Empirical study
Van Dyke, Midha, & Nemati, (2007)	X			Increased privacy empowerment leads to a reduction in privacy concerns and increased privacy trust.	Empirical study
Ren & Lou (2008)			X	Designed an authentication and key agreement protocol for users' privacy protection.	Experimental study
Koslov et al. (2010)			X	Identification of the security and privacy threats attributable to IoT devices	Qualitative study
Brush et al. (2011)			X	The design of home automation systems should be simplified to enable users to be able to control their settings for privacy protection.	Qualitative study
Xu et al. (2011)	X	X		Identification of the major areas in which previous research contributions on privacy concerns reside and the	Qualitative study

Researchers	Research Focus			Findings on Privacy Issues	Methodology
	Online[1]	Mobile (LBS[2])	System Design		
				Relationship that exists between information privacy and other constructs.	
Weber (2011)			X	Creation of a stable legal framework can help protect users' privacy and security in IoT devices.	Qualitative study
Wakefield (2013)	X			Positive mood-enhancing website features will effect users' website trust & privacy beliefs to motivate online transaction.	Experimental study
Li (2014)	X			Disposition to privacy has a positive impact on online & website privacy concern.	Empirical study
Notra et. al (2014)			X	Security & privacy compromise of some home automation systems with ease hence the proposal of a network level solution to protect users.	Experimental study
Sadeghi et. al (2015			X	Cybersecurity & Privacy framework is required to protect of IoT from privacy invasion.	Qualitative study
Keith et. al (2016)		X		Integrating a privacy assurance system significantly influenced the adoption of mobile applications & information disclosure.	Experimental study
Pishva (2017)	X			Proposition of an appropriate security and privacy model that can counter the numerous attack scenarios associated with online transactions via smart appliances.	Qualitative study

Researchers	Research Focus			Findings on Privacy Issues	Methodology
	Online[1]	Mobile (LBS[2])	System Design		
Han et. al (2018)			X	Proposal of a new cognitive approach that enables near-complete privacy protection for location-based service (LBS) users using a multi-server architecture that cuts off the direct connection between the LBS queries and the query issuers	Experimental study
PeD approach to HAS[3]			X	Evaluate user behavior to privacy concern when privacy is embedded in home automation systems.	Empirical study

Summary

Although the foundation for this research study has been established based on previous studies, it is aimed at expanding on those studies to investigate how users' behavior is impacted by the use of emerging technology of the home automation system which are not only invasive but also tend to compromise users' privacy.

This chapter presents an overview of the review of past literatures related to this study. The various literatures include the underline theory for the research which is the PCT as well as the specific model relating to this research. The theoretical foundation and research model were based on the PCT which also incorporates the privacy paradox concept and the theory of bounded rationality. This is aimed at evaluating the tradeoff of privacy and the benefit beliefs that would influence a user's behavior in home automation usage for the anticipated benefits while ignoring the associated privacy concern. Based

[3] Privacy embedded Design (PeD) approach to Home Automation Systems (HAS) – focus of this research proposal.

on the research questions presented in the previous chapter, hypotheses were developed as well as a research model. An overview of past literatures relating to the constructs in the research model including the various research methodologies used in previous studies have also been presented.

The theory development was an attempt to evaluate how the antecedents (privacy embedded design and privacy self-efficacy) to privacy concern impact on the home automation usage as an outcome. The chapter also provide an overview of some security and privacy challenges associated with the home automation system and what previous researchers have proffered as solutions to these challenges. The security and privacy challenges associated with IoT and especially the home automation systems were also reviewed in this chapter with an attempt to explain why the home automation systems is prone to these challenges based on their design features.

The literature review is aimed at assessing the previous studies related to this research and the existing gaps that this study would attempt to fill in the body of knowledge of IS security and privacy field. The chapter thus provided some insight into the areas of previous research that had studied various aspect of user behavior to privacy concern and what the focus of these studies were.

Chapter 3

Methodology

Introduction

The focus of this research is a quantitative analysis using empirical study to assess the mediating effects of privacy concern on the relationship between privacy embedded design and home automation usage as well as on the relationship between privacy self-efficacy and home automation usage. The model developed for this study and the hypotheses were tested for this mediation effects using the partial least square structural equation model (PLS-SEM). The PLS-SEM analysis is suitable in this study because the result of the test either confirms or disproves the underlying theory adopted for the study (Hair, Hult, Sarstedt & Ringle, 2017). The exploratory analysis was also applied to the data set in order to further explore the relationship between the variables. Exploratory study is valuable here because it provides a means of asking questions in order to help discover more insights about the topic under consideration and the constructs used in the study (Lewis, Saunders & Thornhill, 2016). The survey strategy which is usually associated with deductive research approach was used for this research study (Lewis, Saunders & Thornhill, 2016). This strategy was used to empirically test the data sourced from anonymous online questionnaires collected from individual participants through the google web survey.

Research Design

The research deployed a quantitative method using a survey with the main data collection method being the online questionnaire was sent to participants through their emails. The benefits associated with this data collection method makes it appropriate to be used for this research.

The use of questionnaires enables the collection of standardized data and also foster easy comparison as well as being a strategy that is perceived to be comparatively easy both to explain and to understand (Lewis, Saunders & Thornhill, 2016). Prior to the survey for the research, a preliminary interview[4] was conducted with selected users of home automation systems to obtain their perspectives about the associated privacy concerns and the viability of the research to be conducted. The interview with ten participants was an unstructured interview aimed at highlighting some preliminary issues that helped in determining the factors that requires further investigations (Bougie & Sekaran, 2013) about the home automation usage and their attendant privacy issues. The interview was conducted at the initial stage of the research planning and was used to direct the focus of the questions in the questionnaire. The following are sample of questions that was asked during the preliminary interview phase:

- What do you understand about home automation system?
- What type of home automation do you use?
- What are the reasons for using the home automation system that you use?
- Do you have any security or privacy concerns about using the home automation system?

[4] The preliminary interview was conducted at the idea paper stage of the dissertation before proceeding to the dissertation proposal stage.

- Do you have an understanding about how the home automation system works?
- Are you aware of any potential privacy issue associated with the home automation system?

The participants for the research was asked to anonymously complete the survey instrument consisting of questions based on their use of the home automation system and the answers to these questions was based on the Likert 5-point scale.

Instrument Development and Validation

Prior studies discussed in the preceding sections of this paper on the APCO model, have provided guidance and baseline which can be built upon and the scales for this study were developed using the standards provided for scale development in selecting the items. The privacy self-efficacy and privacy concern constructs for the model for this study have been widely used comprehensively by previous researchers. The privacy self-efficacy and the privacy concern items were adapted from Dinev and Hart (2006), Dinev and Hu (2007), and Smith et al. (2011). The privacy self-efficacy items measure users' ability to use the privacy settings in the home automation systems, while the privacy concern items assess users' view of the privacy issues associated with the use of home automation system.

Survey items for the privacy embedded design construct were designed to measure users' understanding of the privacy settings of the home automation system and were an adaptation from Spiekermann (2007) and Spiekermann (2012). The home automation usage survey items were also adapted from the works of Ormond, Warkentin, Johnston, and Thompson (2016) as well as that of McKnight, Choudhury, and Kacmar (2002). The items were aimed at measuring users' behavior towards the use of home

automation systems. Although the items are more tailored for home automation usage, they align well with the items developed by these prior researchers for website usage in e-commerce transaction and meet the needs for the study (Bhattacharjee, 2012). The survey items were however tested for both reliability and validity to ensure that they actually measure the constructs they have been adapted for (Bougie & Sekaran, 2013).

Reliability is the degree to which a survey items are dependable in measuring the construct they are set up to measure (Bhattacharjee, 2012). The internal consistency reliability test which is a measure of the consistency between different items of the same construct was adopted to test for reliability and was determined by using the traditional Cronbach's alpha calculations to assess if the acceptable values were reached for the scale items. The Cronbach's alpha provides the estimation of reliability based on the intercorrelation of performance on each item with overall performance across the indicator variables (Hair et. al., 2017).

The Likert 5-point scale was used for the survey items as suggested by Gay, Airasian and Mills, (2009) because the use of the Likert scale makes the Cronbach's alpha a more useful option to assess the reliability of internal consistency. This 5-point integer scale was designed to examine the extent to which the respondents agree or disagree with a statement (Bougie & Sekaran, 2013). The five-point scale has been proven to be a good scale and increasing the rating scale to seven or nine point does not necessarily improve the rating reliability (Bougie & Sekaran, 2013). The items on the scale were measured with ranges from "1" = Strongly Disagree to "5" = Strongly Agree. This coding parameter helps to approximate the interval-level measurement required for

the research variables to be used in SEM and thus fulfill the requirement of equidistance (Hair et al., 2017).

Following the initial development of the survey items based on literature, a group of expert panel provided feedback based on their review of the survey items and the survey was revised to adjust for rewording, re-phrasing, missing words, and restructuring. A pilot testing of the survey was subsequently conducted based on the revised instrument and this was further reviewed and adjusted based on the result of data analysis of the revised survey. The final data collection was based on the revised instrument and Table 2 provides an overview of the revised survey items.

Table 2

Survey items for evaluating user behavior when privacy is embedded into the design of home automation systems.

Constructs	Item Code	Lead Questions	Literature
Privacy embedded Design	PeD 1	My home automation system has privacy embedded into them.	Adapted for this study from: Spiekermann, (2007); Spiekermann, (2012).
	PeD 2	I can easily locate the privacy settings on my home automation system.	
	PeD 3	The user guide that accompany my home automation system contains information about privacy settings.	
	PeD 4	The user guide for my home automation system provides a step by step guide on how to use the privacy settings of the device.	
	PeD 5	The user guide for my home automation system encourages me to change the privacy settings of the device before use.	

Privacy Self-Efficacy	PSE 1	I am confident of easily locating the privacy settings of my home automation system.	Adapted for this study from: Dinev & Hart, (2006); Dinev & Hu (2007); Smith et al. (2011).
	PSE 2	I can confidently operate the settings of my home automation system.	
	PSE 3	I am confident about selecting the appropriate privacy settings for my home automation system.	
	PSE 4	I understand what the privacy settings of my home automation systems represents.	
	PSE 5	I know the appropriate privacy settings to select in order to protect the privacy of my home while using the home automation system.	
Privacy Concern	PC 1	I am of the opinion that the use of home automation system creates a privacy concern.	Adapted for this study from: Dinev & Hart (2006); Dinev & Hu (2007); Smith et al. (2011).
	PC 2	I am of the opinion that the use of home automation system increases the chances of violating the privacy of the home.	
	PC 3	I am concerned that using the home automation system will cause the privacy of my home to be invaded.	
	PC 4	Including privacy settings in home automation systems will provide assurance of privacy for home automation usage.	
	PC 5	Understanding how to use the privacy settings of my home automation system will reduce my privacy concern.	

Home Automation Usage	HAU 1	I currently use or plan to use the home automation system.	Adapted for this study from: Ormond et.al., (2016); McKnight et.al., (2002).
	HAU 2	I will prefer to use a home automation system that has privacy settings included in the device.	
	HAU 3	I will prefer to use a home automation system with a default privacy setting set to protect the privacy of my home.	

Validity is the extent to which the survey items used adequately measure what they are intended to measure in the underlying construct they are supposed to measure (Bhattacharjee, 2012). The construct validity and content validity were conducted for the survey items. Construct validity was used to establish the extent to which the results of the tests are related to the underlying set of variables that is being tested in the research model (Hair et. al., 2017); while content validity was used to assess the extent to which the survey items matches the relevant content domain of the construct they have been identified to measure (Bhattacharjee, 2012). The content validity of the survey items was established by relying of the judgement of the expert panel of judges who are professionals in research, information system security and information privacy (Bhattacharjee, 2012); while factor analyses was employed to assess the convergent and discriminant validity of the construct items (Hair et. al., 2017).

Ethical Consideration

In other to be compliant with the ethical consideration of the research as stipulated by the Institutional Review Board (IRB) of Nova Southeastern University, the IRB process was strictly adhered to and their approval was obtained before the

commencement of the research study. The survey participants were notified and made to proceed with the survey on a voluntary bases through their approval on the consent form that preceded the questionnaire and that they were made to understand their willingness to opt out of the survey whenever they choose to without any penalty. The participants were also be assured of the anonymity of their response and the protection of any personal information provided during the process in accordance with the applicable privacy regulations such as the GDPR, the Canadian and the USA privacy regulations.

Population and Sample

Researchers often used different methods to determine the sample size of participants in a research; for example, a power of 80 percent for a maximum of 5 percent standard error biases for which power is assessed is a commonly acceptable value for sufficient power (Muthén & Muthén, 2002). In addition, Fidell (1996) provided a general rule of thumb of 300 participants to be used in determining the sample size for factor analysis. Moreover, having a large sample size increases power and decreases estimation error but due to factors like financial costs and time, sample size is mostly reduced (Cohen, 1992). Hence generating a sample size that is adequate enough to provide sufficient power and also allows for easy collection helps to create a good balance (Morgan & VanVoorhis, 2007).

The correlation analysis for this study requires the use of a significance tests at 5 percent (α=.05) probability of error and the sample size needed to detect a medium effect size at an 80 percent statistical power is 67 (Cohen, 1992, page 4). However, in order to reduce the possibility of a type II error (i.e. not rejecting the null hypothesis that is false – 'false negative') and to avoid a type I error (i.e. rejection of a true null hypothesis – 'false

positive'), a sample size of approximately100 participants have been found to be adequate (Hair, et.al, 2017). The final sample size after the data was screened and reviewed for missing data for this study was 313 participants out of the 330 respondents. The respondent value amounts to approximately 47% of the 700 distributed online survey. The online survey participants were a mix of adult users and non-users of home automation systems from around the Eastern and Western Canada.

Data Analysis Method

The partial least square for structural equation model (PLS-SEM) method for data analysis was adopted to analyse the data collected in this study. This method of data analysis is appropriate for this type of research as it helps to establish the causal model that was predicted for the study through a mediation process (Hair et al., 2017). Additionally, PLS-SEM is considered appropriate for research studies with sample size and complex models as obtainable in this research (Hair et al., 2017). Further, the application of PLS-SEM to a wide variety of research situation also includes the benefits of its high efficiency in parameter estimation as shown in the greater statistical power exhibited by this method, hence their preference by researchers (Hair et al., 2017).

The causal model that has been developed and presented in figure 1 was tested to ensure an appropriate model fit is established using SEM whereby the fit indices indicates that the model is a representation of the data. The mediation tests that helps determine if all the hypotheses in the model are supported (Hair et al., 2017) was tested using the PROCESS macro installed into the IBM SPSS. To test the applicability and validity of the instruments in this study; the exploratory factor analysis (EFA) which is a classical approach for establishing construct validity was used to demonstrate the

evidence of convergent and discriminant validity of the instruments (Bagozzi, Phillips & Yi, 1991). While the evaluation of the internal consistency reliability of the scale items for each construct deploys the traditional Cronbach's alpha, which provided an estimate of the reliability based on the intercorrelations of the observed indicator variables (Hair et al., 2017).

With the EFA as a useful tool in discovering potential latent sources of variation and covariation in observed measurements, it is expected that scales with good measurement properties should exhibit high factor loadings or "converge" on the latent factors of which they are indicators; conversely, these same indicators should also exhibit small loadings on factors that are measured by differing sets of indicators (Grover & Segars, 1993)**.** The results obtained from this data analysis correspond to the underlying theoretical constructs presented in figure 1 above (Grover & Segars, 1993). The Hayes (2017) PROCESS macro for SPSS was used to analyse the mediation effects of the mediator on the variables as depicted in the research model in figure1. The PROCESS macro in SPSS was used for assessing the effects of mediation because it has been proven to be a better evaluator of these effects than other tools (Hayes, 2012). The traditional tools often used has been found to be insufficient in providing the methods that researchers are currently advocating for modern mediation and moderation analysis as well as their integration (Hayes, 2017).

One advantage of the PROCESS tool for assessing mediation effects is the fact that it eliminates the requirement by analysts to engage in several variable transformations and sometimes write codes that are customized to their data and problems in other to achieve the results of mediation or moderation effects (Hayes,

2012). This is a process that can be both time consuming and prone to error for those who are not conversant with these methods (Hayes, 2012) as such, PROCESS macro for SPSS have combined many of the functions of other popular tools used in IS research into a simple and easy-to-use procedure, thereby eliminating the need for researchers to learn multiple tools to assess the effects of mediation (Hayes, 2017). Another advantage of this tool is also the fact that it 'allows mediators to be linked serially in a causal sequence rather than only in parallel, offers measures of effect size for indirect effects in both single and multiple mediator models, and offers tools for probing and visualizing both two and three way interactions' (Hayes, 2012. Pg. 3). These advantages make the PROCESS macro tool exceeds the capabilities of other tools and thereby useful in this research to better evaluate the relationships between the outcome (dependent variable) and the other independent variables while taking into consideration the effects of the mediating variable.

Result Presentation

The presentation format of the research dissertation report is according to the procedures as prescribed in the Nova Southeastern University Dissertation Guide for the Doctoral students of the College of Computing and Engineering. The results of the research were presented in a format that makes it easy to be interpreted by the target audience. The analysed data results from all the analyses including the tables and figures of outputs are presented in the appendices as well as the results of the data output obtained from the PROCESS macro for SPSS. The results of the reliability and validity tests are presented in a tabular format while the sample of the survey questionnaire used for data collection and the approved IRB are also presented in the appendices.

Resources Requirements

The resources that were used to complete this research include a Wi-Fi-enabled computer system such as a laptop with a Microsoft office suite and data analyses software such as IBM SPSS, SmartPLS and the PROCESS macro installed into the SPSS. The data analysis software was required for the data analyses, interpretation, and presentation, while the Microsoft word was used to compile the result of the analysis and the Microsoft Visio used to draw the research model illustrations. Books, unlimited access to peer-reviewed journals and articles as well as other credible publications were used to conduct this study.

The study relied on the Alvin Sherman Library of the Nova Southeastern University to obtain most of the publications and the online google forms was leveraged to administer the online survey questionnaire which is the instrument for data collection. The requirement for the use of human participant in a research include the IRB approval, and the process was completed, and appropriate approval obtained before the commencement of the research study. The research results were presented in accordance with the Nova Southeastern University Doctoral Dissertation Guide for the College of Computing and Engineering.

Summary

The chapter outlined the approach of the research as well as the method of data collection and analysis. The study is a quantitative research with the use of survey questionnaire as the data collection instrument. It also explained how the instrument reliability and validity were established in the research. The resources required for the study were outlined as well as the software needed for the data analyses. The data

analyses methodology adopted were the use of IBM SPSS, SmartPLS and the PROCESS macro for SPSS tool. The chapter also highlighted the advantages and basis for the choice of analyses tools as well as how the results of the various analyses are presented in the dissertation report.

Chapter 4

Results

Overview

This study was conducted with the aim at examining the impact of embedding privacy in the design of home automation system on home automation usage based on a quantitative approach that uses 5-Point Likert scale (Appendix A) for data collection. The study seeks to provide answers to the research questions for the study as well as test the hypotheses that predicts the impacts of privacy embedded design and privacy self-efficacy on home automation usage while being mediated by privacy concern. This study adopts the Partial Least Square Structural Equation Modelling (PLS-SEM) approach which is most suitable for prediction-based research (Hair et. al., 2017). The PROCESS macro for SPSS (Haye, 2012) was also used to test the mediation effects of the hypotheses.

The preliminary tests of the collected data for descriptive statistics, normality, reliability and validity was conducted using the IBM SPSS tool while the Smart PLS tool was used to conduct the structural equation modelling (SEM) data analyses and the PROCESS macro installed into IBM SPSS was used for the in-depth evaluation of the mediation effects of the structural model. This chapter presents the results of the various analyses as well as the discussion of findings of the results.

Preliminary Tests

In order to ensure the validity and reliability of the newly developed scale items in the study, a pre-testing is necessary (Sekaran & Bougie,2013). The questionnaire was presented to a group of expert panels which comprises of professors in the field of information systems security, professors in the field of information privacy as well as technical experts in security and privacy. The panel also include research experts with little or no technical expertise in systems security or privacy in other to have a comprehensive assessment of the content validity of the survey items. Based on the experts' review some of the scale items wordings were re-assessed while an item was corrected for negative wording.

A pilot study was subsequently conducted with 30 participants who provided feedback on the survey items. The participants consist of colleagues, friends, neighbors, and other professional associates. Some of the feedback provided by the participants include suggestions on the use of response button instead of checkmarks to prevent double response on a question. Another feedback was also to make the survey link open as opposed to it requesting for participant's emails before they can access it as this might discourage some participants from completing the survey. All of these feedbacks were incorporated and necessary adjustments made on the survey items before the final draft was sent out.

Data Collection

The Data collection was conducted by sending the survey link to target participants who are users and potential users of home automation systems through emails, WhatsApp messages, and Facebook posts. The collection was carried out for a

period of about three weeks between March and April 2020 and an approximate response rate of about 47% (330 responses) was achieved from the 700 target participants that the link was sent to. This was impressive as it is well over the 30% expected response rate for survey-based studies.

Pre-analysis Data Screening and Descriptive Statistics

Pre-analysis screening is required to check the validity of data prior to analyzing the data. Pre-analysis data screening not only helps to ensure that the data meets the basis of assumption for the analysis to apply but also helps to detect any error or missing values associated with the data before analyzing them (Mertler & Vannatta, 2013). As part of the pre-analysis data screening, the measurement model assessment of the constructs items was conducted to determine their indicator reliability, internal consistency, convergent validity, and discriminant validity as described by Hair et. al., (2017).

The data for the analysis was screened and reviewed for any missing data and the descriptive statistics was used to assess the normal distribution of the data. Descriptive statistics is often used by researchers to describe the characteristics of the distribution of the scores for the collected data. It also shows the attributes of the variables used in the study and provides a good idea of whether or not the collected data meets the various assumptions for the statistical analyses to be conducted (Bougie & Sekaran, 2013). The descriptive statistics used in this study as a measure of describing the data before further analyses are conducted are the standard skewness and kurtosis which was used to examine the normality of the data as presented in Appendix D. Data skewness represents how the responses fall into a normal distribution and kurtosis describes the extent to

which data clusters at the end of the distribution in form of outliers (Field, 2018). The acceptable value for these measures is a level of +/- 1.0 (Field, 2018). The value obtained as shown in the results presented in the appendix is within this range with a skewness value of 1.43 and kurtosis value of approximately 0.6. Despite the skewness value being a little above the acceptable value, it still falls below three times the value of the standard error of skewness which is considered acceptable (Lowry & Gaskin, 2014).

Outliers and Normality Tests

An outlier is an extreme value that is very different from the rest of the data (Field, 2018). To avoid the bias usually associated with the violation of the general assumptions for multivariate statistical testing, the normality, linearity, and homoscedasticity of data should be established (Mertler & Vannata, 2013). Given that multivariate outliers are often difficult to identify, the data sets were first examined for outliers using the Mahalanobis distance procedure through the IBM SPSS tool. The analysis result revealed some outliers out of which an initial three extreme outliers were removed and a total of seventeen outliers were eventually removed from the data sets.

Given that the results of inferential statistical testing may be subject to bias if any of these assumptions are violated, the test for these assumptions were conducted to achieve the robustness required for the level of significance in this study (Kennedy & Bush, 1985). Normality refers to how the data of a particular variable is distributed and one of the ways to measure this is the use of histogram (Field, 2018). The statistical output results and graphs conducted for these tests which include the histogram, Q-Q plot, P-P plot and scatter plot as presented in Appendix D, all show that the data distribution has not violated any of the normality assumptions for multivariate data sets.

Data Analysis

Internal Consistency Reliability

The internal consistency reliability is typically the initial criterion to be established for this type of research and this is assessed by observing the results of the Cronbach's alpha (α) value which is the traditional scale used to measure the internal consistency reliability of measurement scales (Hair, et. al., 2017). Cronbach's alpha provides an estimate that is determined based on the intercorrelations of the observed indicator variables and values above 0.7 is generally acceptable as it depicts a reliable scale and a lower value indicates an unreliable scale (Kline,1999). The '*Cronbach's Alpha if Item Deleted*' column of the test output was used to determine whether removing an item will improve the overall reliability values as values in this column that are greater than the overall reliability value will indicate that removing them will mean an improvement to the alpha value. Additionally, the alpha values also depend on the number of items on the scale, because it can be affected by scale items with reverse wordings (Field, 2018).

The pilot study that was conducted with the initial population of 30 participants of the survey was used to test for the scale reliability by observing the Cronbach's alpha reliability scores and also to conduct some preliminary data manipulations. The Cronbach's alpha was calculated using the IBM SPSS software and the results is presented in Appendix C. All the scale items for the constructs have alpha values that were substantially above the acceptable value of 0.7 except for the scale item of the HAU construct with an extremely low alpha value of 0.379. A review of the '*Cronbach's Alpha if Item Deleted'* column for this scale item, shows that deleting the HAU5 scale item will

improve its alpha value although not significantly. The process of deletion was subsequently applied to two other scale items of the HAU scale items in that column (i.e. HAU3 and HAU4), and the test was re-run to obtain an alpha value of 0.804 (Appendix C4b) which is an acceptable value for internal consistency reliability obtained for the initial pilot study.

Composite Reliability

Composite reliability is often assessed to help address the limitations associated with the Cronbach's alpha as a measure of determining the internal consistency reliability (Hair, et.al., 2017). This measure is determined using the different outer loadings of the indicator variables and varies between 0 and 1 with higher level of reliability indicated by higher values and values between 0.7 and 0.9 considered satisfactory while those above 0.95 are not considered to be desirable (Hair, et.al., 2017).

Table 3

Internal Consistency and Composite Reliability Results

Constructs	**Internal Consistency Reliability**		
	Composite Reliability	Cronbach's Alpha	rho_A
	>.70	**>.70**	**>.70**
Privacy embedded Design (PeD)	.916	.889	.938
Privacy Self-Efficacy (PSE)	.935	.930	1.358
Privacy Concern (PC)	.831	.746	.818
Home Automation Usage (HAU)	.916	.816	.816

The values obtained for the final internal consistency and composite reliability assessment for this study as shown in Table 3 and Appendix H fall within the satisfactory range with all the constructs having values that are greater than the 0.7 threshold.

Structural Equation Modeling

The Smart PLS 3.0 tool was used to perform the structural equation model for this research and all the factors required for an appropriate model was established before proceeding the analysis. The smart PLS tool was chosen for this analysis because it is best suited for assessing the causal effects of a model in a research that is based on PLS-SEM (Hair, et.al., 2017). The SmartPLS was used to perform various tests such as the model fit, construct reliability and validity, discriminant validity and the tests of significance. The results of the initial running of the PLS algorithm enables the identification of item indicators that do not meet the acceptable threshold values of the various tests as presented in Appendix E and Appendix F. Based on the assessment of the result output obtained for this test, five scale items (i.e. PC3, HAU3, HAU4, HAU5, and HAU6) were removed from the model to achieve the acceptable model fit and threshold values.

Goodness of Fit Indices for the Model

Establishing how well an hypothesized model structure fits the observed data is assessed through the goodness of fit indices as it provides an estimate of any error observed in the model as well as identify any discrepancies in the model specification (Field, 2018). The goodness of fit for the model was estimated using the SmartPLS algorithm and Table 4 and Appendix H provides the estimated values for establishing the model fit for this study. Although the standardized root mean square residual (SRMR) is a model fit measure that is often used to assess covariance-based structural equation (CB-SEM) models, it has also been adopted for use in PLS-SEM (Hair et. al., 2017). SRMR is defined as the discrepancy between the observed correlations and the model-implied

correlations (Hair et. al., 2017. Pg. 193). In SRMR, a value of zero represents a perfect fit and values less than 0.08 is generally considered a good fit (Hu & Bentler, 1999). However, as pointed out by Hair et. al. (2017), the 0.08 threshold is considered low for PLS-SEM because the discrepancies associated with this measure play different roles in CB-SEM and PLS-SEM. The SRMR assessment for this research archived the threshold of less than 0.08 as well as the normed-fit indices (NFI) value of greater than 0.90 as recommended by Bentler and Bonnet (1980). Thus, meeting the requirements for model fit indices.

Table 4

Model Fit Indices Results

	Saturated Model	**Estimated Model**
SRMR	.051	.051
d_ULS	.354	.350
d_G	.210	.210
Chi-Square	1694.881	1694.881
NFI	.981	.981

Convergent Validity

Convergent validity measures the extent to which measures correlate with alternative measures of the same construct through the assessment of the outer loadings of the indicators. The Average Variance Extracted (AVE) is commonly used to assess this requirements with the acceptable minimum threshold for the AVE is 0.5 while the standardized outer loadings threshold should be 0.7 at a minimum (Hair, et. al., 2017). The square of the standardized indicators' outer loadings was also used to assess how much of the variation in the outer loading is explained by the construct (Hair, et. al.,

2017). The established rule of thumb is to have a latent variable that explains substantial part of each indicator variance with a value of 40% being the minimum acceptable value (Hulland, 1999).

Table 5

Convergent Validity Results

Variables	**Indicators**	**Convergent Validity**		
		Indicators Loadings	Indicator Reliability (Loadings Squared)	AVE
		>.70	**>.40**	**>.50**
Privacy embedded Design (PeD)	PeD_1	.719	.517	.687
	PeD_2	.817	.667	
	PeD_3	.898	.806	
	PeD_4	.898	.806	
	PeD_5	.801	.642	
Privacy Self-Efficacy (PSE)	PSE_1	.838	.702	.744
	PSE_2	.822	.676	
	PSE_3	.826	.682	
	PSE_4	.885	.783	
	PSE_5	.936	.876	
Privacy Concern (PC)	PC_1	.660	.440	.553
	PC_2	.681	.464	
	PC_4	.853	.728	
	PC_5	.765	.585	
Home Automation Usage (HAU)	HAU_1	.922	.850	.845
	HAU_2	.916	.839	

Having initially obtained a weaker outer loadings through the SmartPLS algorithm, the effects of removal of some items was carefully observed and these items

were removed so as to achieve the acceptable thresholds for all the parameters. As presented in Table 5, Appendix G and Appendix H, the minimum threshold values for the standardized indicator loadings, square of the standardized loadings and the AVE were mostly surpassed. The values of the indicator reliability for convergent validity assessment presented in the table, is obtained by calculating the square of the indicator loadings.

Discriminant Validity

Discriminant validity shows the distinction of a construct from other constructs and helped establish the uniqueness of that construct when compared with other construct in the model (Hair, et.al., 2017). This is typically first established through the assessment of the outer loading on the associated construct which should be greater than any of its cross-loadings or correlations on other constructs (Chin, 1998).

Table 6

Discriminant Validity Results

Variables	**Discriminant Validity**	
	Fornell-Larcker Criterion **>.70**	HTMT Confidence Interval does not include 1
Home Automation Usage (HAU)	.919	Yes
Privacy Concern (PC)	.744	Yes
Privacy Self-Efficacy (PSE)	.863	Yes
Privacy embedded Design (PeD)	.829	Yes

The test results obtained for the discriminant validity of this study show that the cross-loadings of each of the associated construct is greater than any of its correlations on

other constructs as provided in Table 6 and the Fornell and Larcker (1981) output results for discriminant validity provided in Appendix H.

Mediation Effects of the Structural Model

The basis of a mediation model is a situation in which the independent variable (*X*) influences a dependent variable (*Y*) directly and indirectly through a mediator (*M*) that is causally located between *X* and *Y* (Baron & Kenny, 1986). The hypotheses for mediation suggest that the relationship between the independent variables and the dependent variable is not a direct effect but operates through a reduction in the mediator (Baron & Kenny, 1986). Hence, for the mediation hypothesis to be true and for mediation to be established in a model, the following four conditions have been specified by Baron and Kenny (1986). (1) The independent variable which serves as the predictor must be significantly related to the mediator. (2) the independent variable must predict the mediator, (3) the mediator must predict the dependent variable and (4) the relationship between the independent variable and the dependent variable should be smaller with the introduction of the mediator to the model as opposed to when it is not.

Taking a clue from Dinev and Hart (2006), the mediation effects of privacy concerns was tested separately using a different tool which also employs the bootstrap-based method. Given that causality which is the bedrock of mediation cannot be tested using the traditional SEM, the bootstrapping-based method of testing the causal effects of mediation was employed in the study as recommended by Hair, et.al., (2017). The PROCESS macro installed into the SPSS was used as a preferred bootstrapping method for analyzing the mediation effects because it offers the unique advantage of linking mediator together in a serial causal sequence rather than only in parallel. It also provides

an output that is necessary to assess the effect size and confidence intervals of the direct effects, indirect effects, and the total effects, all of which are required for adequate and seamless mediation analysis (Hayes, 2017).

Total, Direct, and Indirect Effects of the Constructs

Mediation effect in a model can be derived from the following equation as proposed by MacKinnon and Dwyer, (1993).

(1) $Y = i_1 + c\ X + e_1$

(2) $Y = i_2 + c'\ X + b\ M + e_2$

(3) $M = i_3 + a\ X + e_3$

Where 'Y' is the dependent variable, 'X' is the antecedent variable and 'M' is the mediating variable. The coefficient *c* represents how strongly 'X' predicts 'Y' while *c'* is the strength of prediction of 'Y' from 'X' while controlling for the strength of the relationship from M-to-Y. the value of *b* is the coefficient for the strength of relationship 'M' and 'Y' while controlling for the strength of X-to-Y relation. The value *a* is the coefficient representing the strength of the relationship between 'X' and 'M'. the part of the relation that cannot be predicted is represented by e_1, e_2, and e_3 while i_1, i_2 and i_3 represents the intercept in each of the three equations.

The value of the *c'* in the second equation above represents the direct effect of 'X' on 'Y' through 'M' and it quantifies the amount by which two cases differing by one unit on 'X' are estimated to differ on 'Y' without considering the effect of 'M' on 'Y'. The estimation of the indirect effect of 'X' on 'Y' through 'M' is through *a b* which is the product of the effect of 'X on 'M' (*a* in equation 3, above) and the effect of 'M' on 'Y' while controlling for 'X' (*b* in equation 2, above). This provides an estimate of how "the

value of two cases differing by a unit on 'X' are estimated to differ on 'Y' as a result of the effect of 'X' on 'M' which in turn affects 'Y'" (Hayes, 2012. Pg. 6). The assessment of the total effects can be achieved through equation (1) above which is the regression of 'Y' on 'X' alone without 'M' and this total effect is represented by *c* in the equation. Therefore, the inclusion of the mediator 'M' in the model is expected to reduce the value of *c'* as opposed to when the mediator is not included in the model (MacKinnon and Dwyer, 1993).

Given the foregoing, the predicted model for this study suggests that the relationship between the two antecedents (i.e. PeD and PSE) and the outcome (HAU) are not a direct effects but both operates through a reduction in the mediator (PC). Therefore, the direct effect of PeD on HAU is the relationship between them while controlling for PC and indirect effect is the effect of PeD on HAU through PC. Similarly, the direct effect of PSE on HAU is the relationship between them while controlling for PC and the indirect effect is the effect of PSE on HAU through PC.

The direct, indirect and total effects of the model for this study were assessed by examining the output results from the running the PROCESS tool within IBM SPSS and the output results obtained is presented in Appendix I while the relevant values have been reproduced in Table 8, Table 9 and Table 10 of the discussion session below. The indirect effect assessment and the examination of its confidence interval help to determine the degree of mediation through the observation of the β value of the output result and its confidence interval (MacKinnon & Pirlott, 2015). Another parameter used in measuring the indirect effect is the effect size which is measured by the beta (β) value of the analysis output.

Findings and Hypotheses Testing

Using the SmartPLS 3.0 tool, the structural equation model path for the research model was first established and the results of the test of significance performed is presented in Table 7 while the results of the analysis are also presented in Figure 3.

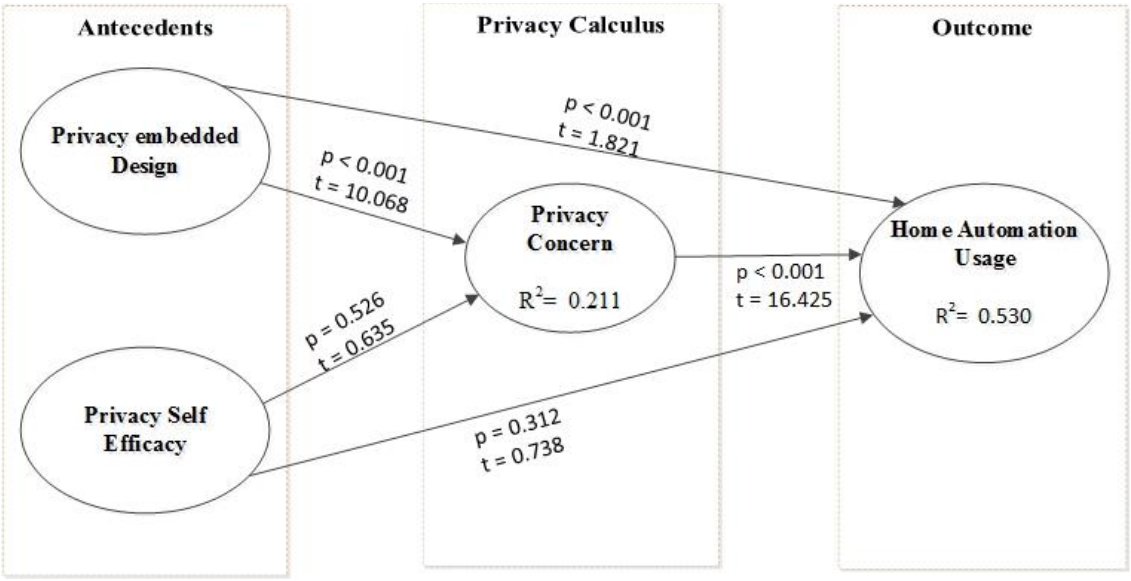


Figure 3. PLS-SEM Results for Home Automation Usage Model

Assuming a 5% significance level, the result shows that most of the relationships in the model are significant except for the relationships **PSE** => **HAU** (p = 0.312), and **PSE** => **PC** (p = 0.526). Given that the research hypotheses and objectives for this study involves a mediation process, the results obtained from the mediation analyses will be used for the hypothesis testing. However, according to Hair et. al., (2017), it is important to first establish the structural model before the mediation effect will be tested as it provides explanations about the causal relationship between the constructs.

Table 7

Result of Structural Equation Model Testing

	Path Coefficients	***t*-Value**	***p*-Value**	**95% Confidence Interval**	**Significance ($p < .05$)?**
PC => HAU	.688	16.425	.000	[.597, .763]	Yes
PSE => HAU	-.020	.738	.312	[-.072, .039]	No
PSE => PC	-.024	.635	.526	[-.089, .490]	No
PeD => HAU	-.069	1.821	.000	[-.152, .001]	Yes
PeD => PC	-.448	10.068	.000	[-.531, -.361]	Yes

The hypothesized mediation relationships among the constructs was tested using the PROCESS macro in SPPS by Haye (2012). The PROCESS macro was chosen as a preferred method because of its simplified method of analysis that do not require further complex calculations and the result presentation that makes it easy for analysis. The output result of the mediation analyses is presented in Appendix I, while Table 8, Table 9, and Table 10 contains details of the analyses. The illustration in Figure 4 forms the basis of the explanations for the results of the research findings.

The basis of the hypotheses for this study is the expectation that privacy concern will serve as a mediator between privacy embedded design and home automation usage as well as between privacy self-efficacy and home automation usage. To assess this mediating role by privacy concern, the illustration in Figure 4 is used in conjunction with the equations 1 to 3 above is used for analysis. Given that this is a simple mediation, the mediation effect on each of the independent variable is assessed separately as recommended by MacKinnon and Pirlott (2015).

Prediction of Mediator by the Antecedents

The result of the linear model of PC predicted from PeD is shown in Table 8 (path *a* in model B of Figure 4) below. The results show that PeD significantly predicts PC (β = -0.245, $p < 0.001$), thereby establishing one of the conditions for mediation stated above. The value of the R Squared shows that PeD explains 15.3% of the variance in PC while the negative sign of the beta coefficients is an indication of the fact that an increase in PeD will lead to a decline in the privacy concern for home automation usage (and vice versa). This supports hypothesis **H1a** of this research. Similarly, the result of the linear model of PC as predicted from PSE is also shown in Table 8 and (path *a* in model D of figure 4). This result also reveals that PSE predicts PC (β = -.065, $p = 0.029$) and also fulfils the mediation condition. The R Squared value also shows that PSE explains approximately 2% of the variance in PC and the fact that the beta value is negative shows the negative relationship that exists between PSE and PC. This does not support this research hypothesis **H2a** which states that: as PSE increases, the privacy concern for home automation usage declines and vice versa.

Table 8

Analysis of the Prediction of Mediator by the Antecedents

	Coefficients (β)	**95% Confidence Interval**	**R^2**	***t*-Value**	***p*-Value**	**Significance ($p < .05$)?**
PeD => PC	-.245	[-.309, -.181]	.153	-7.488	.000	Yes
PSE => PC	-.065	[-.073, -.009]	.015	-2.196	.029	Yes

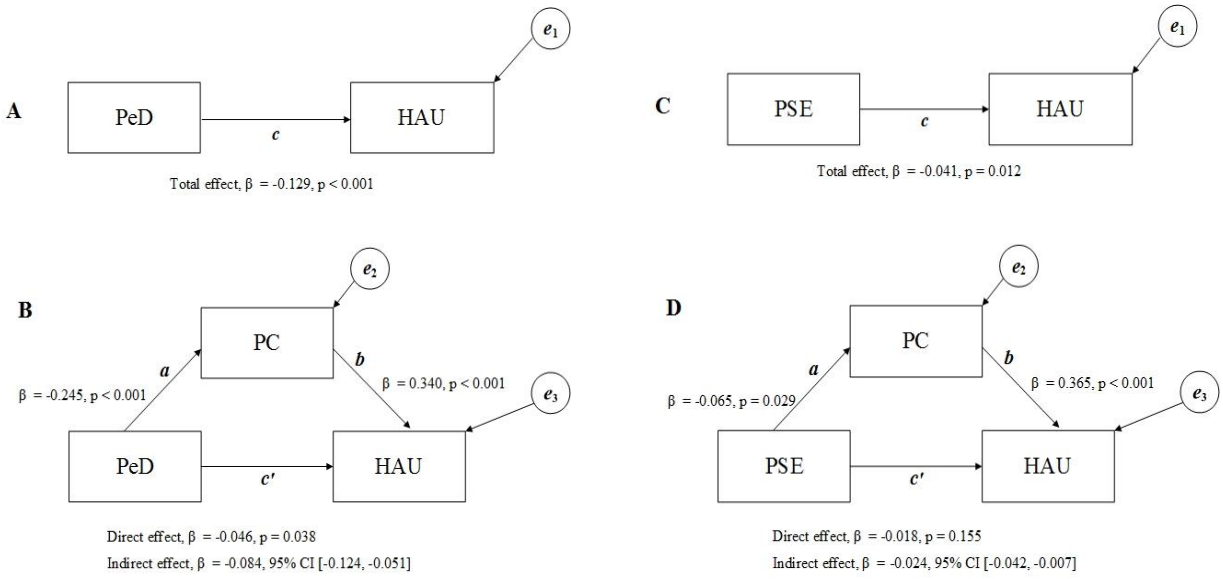


Figure 4. Mediation Effects for Home Automation Usage

Direct and Indirect Effects

The indirect effects of both models were found to be significant for the purpose of our hypotheses testing since neither of the 95% confidence intervals include zero (Table 9 and Appendix I). This indicates that PC actually mediates the relationship between PeD and HAU as well as the relationship between PSE and HAU; thereby supporting the research hypotheses and the objectives of this study.

The results of the direct effects of the mediation is also presented in Table 9 Appendix I. These results show the regression model of HAU predicted from both PeD and PC (path *c'* in model B of figure 4). From these results in Table 9, PeD predicts HAU (β = -0.046) with the inclusion of PC as a mediator, however, the role of PC as a mediator in predicting HAU (β = 0.340) is more significantly. The model also explains 46% of the variance in HAU as depicted by the R Squared value. The *p* value (*p* = 0.004) is

significant at 95% confidence level and therefore supports the hypothesis **H3** of this research study. Given that the *p* values of all the paths in this model are significant, indicating a partial mediation which is also known as complementary mediation (Hair, et.al., 2017). Table 9 also presents the output results (available in Appendix I) for the regression of HAU predicted from both PSE and PC (path *c'* in model D of figure 4). In a similar manner, the results also show that PSE predicts HAU with the inclusion of PC (β = -0.018), however, PC predicts HAU (β = 0.365) more significantly which should be expected as a condition for mediation. The R Squared also shows that the model explains 45% of the variance in HAU while the *p* value (*p* = 0.155) is not significant at 95% confidence level and therefore indicates a full mediation effect and therefore supports the mediation effects predicted for the research hypothesis.

Table 9

Analysis of the Direct and Indirect Effects of the Mediation

	Direct Effect (β)	**95% Confidence Interval of the Direct Effects**	***p*-Value**	**Significance ($p < .05$)?**	**Indirect Effect (ß)**	**95% Confidence Interval of the Indirect Effects**	***p*-Value**	**Significance ($p < .05$)?**
PeD => HAU	-.046	[-.077, -.015]	.004	Yes	-.084	[-.124, -.051]	.000	Yes
PSE => HAU	-.018	[-.042, -.007]	.155	No	-.024	[-.042, -.007]	.000	Yes

Total Effects

The results obtained for the total effects of the mediation is presented in Table 10 and Appendix I. The path of the total effects is also illustrated by *c* in model A and model C of figure 4 above. This is the path between the antecedents and the outcome without

the influence of the mediator. In this study, the paths represent the effect of PeD on HAU as well as the effect of PSE on HAU without PC. As presented in Table 10, for model A, the values obtained for this path show that PeD significantly predicts HAU (β = -0.129) in the absence of the mediator PC and the R Squared value indicates that the model explains 14% of the variance in HAU. The *p* value ($p < 0.001$) is significant at 95% confidence level and therefore supports the hypothesis **H1b** of this study. Similarly, model C of figure 4, shows the effect of PSE on HAU when the mediator PC is not present in the model. The values obtained for path *c* in the model also show that PSE predicts HAU (β = -0.041) and the R Squared value tells us that the model explains 2% of the variance in HAU. The *p* value ($p = 0.012$) is equally significant at 95% confidence level and does not support the hypothesis **H2b** of this study.

Table 10

Analysis of the Total Effects

	Total Effect (β)	**95% Confidence Interval of the Total Effects**	**R^2**	***t*-Value**	***p*-Value**	**Significance ($p < .05$)?**
PeD => HAU	-.129	[-.165, -.093]	.139	-7.089	.000	Yes
PSE => HAU	-.041	[-.073, -.009]	.020	-2.532	.012	Yes

Based on the explanations of the findings provided above, the summary of the results of findings and the corresponding hypothesis as supported by the findings is presented in Table 11 below. The table also include a column for assessing whether the

findings supports the stated conditions that ensures whether or not the mediation effects are valid in this study (i.e. to ensure that mediation actually occurred in the model).

Table 11

Summary of Research Hypotheses and Results

Hypotheses	**Relationship**	**Corresponding Mediation Analysis**	**Results**	**Mediation Conditions Met?**
H1a	Increase in Privacy embedded Design will reduce the privacy concern for home automation usage.	Indirect effect	Supported	Yes
H1b	Increase in privacy embedded design will increase home automation usage.	Total effect	Supported	Yes
H2a	Increase in privacy self-efficacy will reduce the privacy concern for home automation usage.	Indirect effect	Not supported	Yes
H2b	Increase in privacy self-efficacy will increase home automation usage.	Total effect	Not supported	Yes
H3	Increase in privacy concern will reduce home automation usage.	Path '*b*' of model 'B' and 'D' (Figure 4)	Supported	Yes

Post-Hoc Power Analysis

A post-hoc power analysis is typically conducted when the effects of the results is found to be non- significant due to the study not having enough power to detect the significance (Lowry & Gaskin, 2014). When such situation exists, an explicit conclusion cannot be made on the results of findings of the study without first assessing whether or not the power of the study is strong enough to detect the significance (Lowry & Gaskin, 2014). Given that some of the results of the study's analyses were non-significant, the post-hoc analysis was conducted to ensure that the study has enough power to detect the significance of the output before a conclusion is made on these non-significant results.

The analysis was performed using the online Post-hoc Statistical Power Calculator for Multiple Regression by Soper (2020). The calculator requires the input of the values of the number of predictors, observed R Squared, probability level and sample size were used as parameters. A result of 1.00 was obtained and this shows that there is enough statistical power in this study to conclude on the results of the SEM findings. The output of the power analysis result is presented in Appendix J.

Summary

In this chapter, an overview of the process of conducting the research is presented ranging from the tests conducted to validate the survey instrument used for the data collection to the data collection procedures. The various statistical analyses conducted for the research was presented and the steps used in describing the data and validating the instruments used was also presented as well as the results of the findings obtained from the various analysis procedures. The structural modelling process performed in this study was explained in this chapter as well as the analyses required to test the mediation effects

predicted for the hypotheses in this study. The results of the findings were presented in both the tabular format and figures were also presented to illustrate some of the analyses carried out. A detailed explanation of the findings and how they support the stated hypotheses and objectives for this study was also made in this chapter. Following the detailed analysis of the obtained results a post-hoc power analysis test was also conducted to ensure that power of the study is strong enough to make appropriate conclusions on the results of the findings obtained for the SEM. The post-hoc analysis test is necessary for the SEM result outputs because of some non-significant result values obtained in the analysis. The next chapter provides the conclusion drawn from the findings and the implication of these conclusions as well as recommendations for future studies.

Chapter 5

Conclusions, Implications, Recommendations and Summary

Overview

The networking of devices such as home appliances and vehicles that contains electronics, software, sensors in addition to connectivity that allows them to interact and exchange data is generally known as the internet of things (IoT). The intelligence of these networked devices with their attendant convenience further breeds security and privacy concerns that can affect users' behavior. The surging privacy concerns for these connected systems continue to create the need for adequate privacy to be embedded in their design and this cannot be over-emphasized. The findings from this research are used to provide answers to the stated research questions and report on the hypothesis highlighted for testing by this study. Many studies have been conducted previously on the impact of privacy concern on connected systems as well as on the exposure of personal information over the internet, however this study specifically identified the impact of embedding privacy into the design of home automation systems and how this would impact its usage.

This study draws on the privacy calculus theory (PCT) as well as theory of bounded rationality and privacy paradox to predict what the impact will be to the level of home automation usage when privacy is embedded into the design of the home

automation systems while having privacy concern as a mediator. It also predicts the impact of privacy self-efficacy on home automation usage with privacy concern as a mediator. This chapter provides the conclusion of the findings obtained from this research studies based on the previously stated research objectives and hypotheses. It also provides some answers to the research questions of focus for this study. In addition, it provides some implications from the conclusions of the findings to the IS body of knowledge as well as to the practitioners. The limitations of the study have also been highlighted, while preferring some recommendations for future studies.

Conclusions

How will privacy embedded design interact with privacy concern to impact home automation usage? How will privacy self-efficacy interact with privacy concern to influence home automation usage? To what extent does privacy concern influence home automation usage? The findings of this study provide answers to these questions and all of the hypotheses stated for the research were also supported. The findings show that the developed research model supports the conditions required to assess mediation effects which enables appropriate interpretation of the results of findings.

Privacy embedded design is the focus of this research and forms the basis of hypothesis **H1a** of the study which states that: an increase in privacy embedded design will reduce the privacy concerns associated with home automation usage. This hypothesis is in line with the central theme of the study and the basis of the first research question which is ‘How will privacy embedded design interact with privacy concern to impact home automation usage?’. It is interesting to find that the results of the research findings support this hypothesis as it was empirically shown that an increase in the level of

privacy embedded design leads to a decline in the privacy concerns that users have for home automation usage.

Previous researchers have studied the effect of privacy concern on the use of internet connected technologies as well as e-commerce transactions and have achieved similar results in their findings. The research by Tan, Teo and Xu, (2005) on embedding privacy into IT devices to reduce the privacy concerns associated with their usage is one example of such studies. Other related researches that mostly focused on online transactions have been conducted using the PCT and the results of their findings have achieved similar outcome (Bies & Culnan, 2003; Keith, et.al., 2016). Additionally, some researchers have also achieved a similar result with their findings showing a reduction in privacy concern through an increase in what the researchers referred to as the concept of privacy-enhanced technology (Lou & Ren, 2008; Weber, 2010). Based on the empirical results of these findings, it can therefore be concluded that embedding privacy into the design of home automation systems reduce the privacy concerns associated with their usage.

Hypothesis **H1b** states that increase in the level of privacy embedded design lead to an increase in home automation usage. The findings obtained from the results of analysis for this research study also supports this hypothesis. This is in line with several previous researches where a positive user behavior has been shown to exist when privacy features are embedded into technology devices (Keith et. al., 2016; Tan, Teo & Xu, 2005).

The results of the findings do not support hypothesis **H2a** of the study which states that an increase in a user's privacy self-efficacy reduce the privacy concern for

home automation usage and hypothesis **H2b** which states that an increase in privacy self-efficacy lead to the increase in home automation usage. Hence it is concluded privacy self-efficacy reduces the usage of home automation directly and also mediated by privacy concern. The idea that self-efficacy reduces privacy concern has been proposed by several researchers on privacy concern based on the cognitive theory that individuals' belief in their ability to perform a behavior (Bandura, 1997). This concept has been adopted and widely used in IS studies and a study by Hassan, (2006) reveals that context-specific self-efficacy contributes greatly to outcome than general self-efficacy. Privacy self-efficacy as an individuals' beliefs about their ability to protect their privacy (Dinev, et.al., 2012) has been shown by previous researchers to influence privacy concern in a similar way as observed in this research findings (Youn, 2009; Rifon, LaRose, & Choi, 2005). Additionally, the findings of the study by Van Dyke, et. al., (2007) which likened empowerment to privacy self-efficacy also shows that an increase in the perceived privacy empowerment, leads to a decrease in the level of privacy concern exhibited by users of IS artifacts.

Hypothesis **H3**, which is the final hypothesis, states that increase in privacy concern will reduce the level of home automation usage. The results of the research findings support this hypothesis and this is also consistent with previous research studies on privacy as well as the PCT (Dinev & Hart, 2006) which is the base theory for this study. The previous studies have mostly shown the negative relationship between privacy concerns and individuals' behavior to the use of IS devices (Acquisti & Grossklags, 2005; Miao & Yang, 2008; Li, Sarathy, & Xu, 2011) which is consistent with the findings in this study.

Implications and Recommendations

This study offers contributions to the IS security and privacy body of knowledge by filling the existing gaps that exists in literature for empirical studies that focus on the design of IoT devices such that they protect the privacy of users by default. Several studies in IS with regards to privacy concerns have been mostly focused on e-commerce transactions as well as other online activities with the aim of such studies being mostly the protection of personal information (Ferrell, Nowak & Phelps, 2000; Miao & Yang, 2008). The findings from this study also contributes to other existing studies by demonstrating how the embedding of privacy into the design of home automation system impact consumers' behavior towards their usage.

As the use of internet connected devices increase, the growing concern for the adequate protection of privacy and how this can be effectively achieved is also increasing. Today most users of IoT devices continue to use them despite the mounting privacy concerns mainly because they consider the benefits of using them to be far greater than the associated privacy concerns attributed to their use. In particular is the home automation systems which are most times included as part of the features in most modern homes from inception at the construction stage. This often happens without requesting the home buyer to make a choice whether or not such features should be included in their homes in which case the users have little or no control on the use of the devices. Some essential home appliances like the heating ventilation and air conditioning (HVAC) are also now equipped with sensor devices such that they can communicate with other home automation devices without the users' knowledge. This research

complements other studies in IS by proffering recommendations on the need to embed privacy into the design of the home automation systems.

The results of the findings of this study suggests that users will generally prefer to have their home automation systems embedded with privacy features as the manufacturers' default at the time of procurement without requiring additional expertise to achieve these settings. This is given the fact that not many users are privacy savvy or empowered with the appropriate knowledge to operate and use the devices in a way that ensures that their privacy is protected. Previous studies have shown how users of connected devices would prefer to engage the use of devices that provide assurance of the protection of their privacy (Barney & Hansen, 1994, Culnan & Armstrong, 1999). Findings from this study also suggest that embedding privacy into the design of home automation systems would encourage more users to gravitate towards its usage as this will provide them with some form of privacy assurance. In addition, designers of these devices can also ensure that the necessary information required to guide users on privacy settings to protect their privacy is included in the user guide of their devices. This will enable users to be empowered to control the privacy of their home environment through appropriate privacy settings.

The findings from this study equally supports the research hypothesis which states that an increase in privacy self-efficacy leads to an increase in the home automation usage. This is in line with how the PCT is used to explain privacy paradox and bounded rationality exhibited by users (Dinev & Hart, 2006; Xu et al., 2011). Based on the cost benefit trade-offs associated with the privacy calculus theory, studies have shown that users of IS devices who are concerned about the invasion of their privacy still engage in

the use of devices that could violate the protection of their privacy (Brown, 2001; Caudill & Murphy 2000; D'Souza, & Phelps, 2009; Hann, Hui, Lee & Png, 2007). However, for most users, the benefits of using the devices far outweighs any associated privacy concerns they might have towards the use of such devices (Kokolakis, 2017; Lee et al., 2013) thereby bringing the theory of privacy calculus into play. Given the complexity of users' privacy behavior towards modern technology, the implication of this findings to the practitioner is that designers of these devices should incorporate privacy protection features into the devices in such a way that consumers of such technology have the ability to manage their own privacy trade-offs even when they have little or no privacy self-efficacy. Thus, ensuring some level of privacy assurance for the protection of privacy while using the devices.

Another beneficial implication for practice as a result of this research is the need for adequate regulations by policy makers that is focused on ensuring that IoT devices meets certain prescribed standards of privacy protection before the devices are allowed to be sold. This is in line with previous studies that had proposed that online service provider ensure the privacy protection of the consumers of their services and provide this assurance through their various privacy statements (Dinev, McConnell & Smith, 2015; Van Dyke, et. al., 2007). The use of internet connected devices can be considered in the same context given that majority of these devices operates using the internet and the information gathered by these devices are often times sent to the servers of the manufacturers which they sometimes use for other purposes without the consumers' consent (Keith, et. al., 2016). Having the regulation in place can help to check these

practice and hopefully ensure that users' privacy is not invaded when they use the devices.

Limitations and Future Studies

This research is limited in scope in that it was restricted to what the impact would be to users when privacy is embedded into the design of home automation systems. The empirical study uses privacy concern as a mediator and does not include any covariates factors, that could influence home automation usage. This could be a limitation as the presence of covariate factors might yield interesting findings that this study did not reveal. Recommendations for future research is therefore proposed for the inclusion of covariate factors into the structural model to determine how other factors other than the antecedents to the mediator used in this study will impact on the outcome of the study.

Despite the credibility of the various methods of analyses and tools used in this study, to ensure that the scale items used are valid and reliable, there is still the possibility of errors associated with their measurement which might cause a limitation to the study. Another limitation is with regards to the web-survey which may be subject to self-selection bias (Parker & Rea, 2014) whereby only participants with good knowledge of the subject provided adequate response to the survey questions. Additionally, the model used to predict the outcome of this research is consistent with the APCO model which uses the PCT as its foundation by considering the antecedents to privacy concern and the consequent outcome based on user behavior (Dinev & Hart, 2006). The PCT holds that individuals would often maximize their benefits by minimizing the associated risks (Dinev & Hart, 2006). This may not always be the case for all individuals.

The antecedent factors to privacy concern for home automation usage (outcome) used in this study are the privacy embedded design and privacy self-efficacy. Given that several other antecedents factors to privacy concern could be responsible for the outcome displayed by individual users of modern technology (Davis, 1989; Venkatesh et al., 2003; Yzer, 2017), and for home automation usage in particular; models that incorporate other antecedent factors to privacy concern for home automation usage will contribute immensely to the pool of researches in the IS body of knowledge. In addition, research that include other variables into the model is also recommended as several factors have the potential to influence the use of home automation systems. The focus of this research is on home automation systems which is just one of the several IoT devices. Similar research with other IoT device might reveal some interesting findings given the prevalent use and the widespread privacy concerns associated with the use of these devices.

Finally, the data collection is restricted to users of home automation system in Eastern and Western Canada. Therefore, the result of the findings in this research study cannot be generalized. It is therefore recommended that extending this work by collecting data from other jurisdictions will be useful for future studies to obtain a broader perspective of the central theme of the study.

Summary

This study was conducted to identify the privacy concern implications associated with home automation usage. An empirical assessment was therefore performed on what the impact would be for home automation usage when privacy is embedded into their design while leveraging on previous literatures and theories. Borrowing from the work of Dinev and Hart (2006), the study used the idea behind the APCO model to predict the

level of home automation usage despite their attendant privacy issues. The study uses privacy self-efficacy and privacy embedded design as the antecedent factors to privacy concern. The goal of this study is to use the PCT and the privacy paradox to assess the level of home automation usage when antecedents to privacy concerns are incorporated. To conduct the study, a set of research questions were presented in conjunction with a developed model and hypotheses were also formulated.

An extensive review of past literatures was carried out to highlight the works of previous researchers with regards to privacy concerns associated with use of modern technologies and IoT devices. The study relied on the PCT as well as the theory of bounded rationality and privacy paradox which have been used by previous researcher for similar studies. The PCT is an adaptation of the beliefs and behavior associated with theory of reasoned action and theory of planned behavior (Dinev & Hart, 2005). These theories have been commonly used by researchers to evaluate users' behaviour where risks and benefit beliefs regarding privacy concern is involved.

The methodology chapter provides detailed information on the research design adopted for this study where the use of a quantitative study approach through a web-based survey was highlighted. The survey instrument was based on a 5-point Likert scale which was first validated by a panel of experts before distribution. The pilot study that was conducted ensures the reliability and validity of the survey instrument in order to detect and correct any errors in the survey items before the final distribution of the survey questionnaires. The link to the google-based anonymous web survey was sent to about 700 potential participant through emails, SMS, WhatsApp messages, and Facebook platform. A response rate of over 40% was obtained with 330 participants proving their

responses. This surpassed the acceptable response rate of 30% which was anticipated for the study (Sekaran & Bougie, 2013).

The tools used for the data analyses include the IBM SPSS v.26, SmartPLS 3.0 and the PROCESS macro which was installed into SPSS and both the descriptive and inferential statistical tests were conducted for the study. A pre-analysis screening of the data was conducted before conducting the main analyses. This was meant to ensure that there were no missing data and a total of 17 observed extreme outliers were removed. The normality and linearity tests were also performed on the data to ensure that none of the assumptions of normality is violated before the main analyses was conducted. The model for the study was tested to ensure that its fitness indices are within the acceptable threshold levels for this type of study. All of the prescribed thresholds required to ensure internal consistency and component reliability, convergent and discriminant validity of the constructs were met before proceeding with further analyses. The structural equation model for measurement model evaluation was performed using the SmartPLS algorithm and the mediation effects required to test the research hypotheses based on the research questions was conducted using the PROCESS macro installed into the IBM SPSS analysis software.

The interpretation of the results of findings were made as presented in chapter 4 and the appendices of this report and results of the analyses were used to conclude on the stated research hypotheses as well as to provide answers to the research questions. The outcome of the finding is consistent with previous researches that show how users react to the privacy concerns associated with home automation usage. The study was concluded by providing discussions on the implications of the research findings, as well

as recommendations both to the IS body of knowledge in information security and privacy as well as for practitioners. Finally, the limitations of the study were highlighted and suggestions for future studies were provided.

Appendix A

Survey Questionnaire

College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

Participant Letter for Anonymous Surveys

NSU Consent to be in a Research Study Entitled
Smart Privacy for IoT: Privacy embedded Design for Home Automation Systems

The person conducting this research is Love James, a doctoral student at the College of Computing and Engineering at Nova Southeastern University and working with Dr. Ling Wang as my supervisor.

You are being asked to participate in this research study and provide your input because you are a user or have a plan to use the home automation system.

The purpose of this study is to find out through an empirical evaluation, users' behavior when privacy is embedded in the design of home automation systems. Home automation systems in the survey refers to any equipment or gadget used in the home that could be controlled or operated through any form of internet connection, Bluetooth, or any other form of sensor connectivity. Examples are smart thermostat, smart fridge, coffee maker, home camera, home virtual assistance, etc.

You will be taking a one-time anonymous survey, which will take approximately 15 minutes or less to complete.

This research study does not involve any anticipated risks to you. To the best of our knowledge, your participation in this research survey have no risk of harm associated with it.

You can decide not to participate in this research and it will not be held against you. You can exit the survey at any point during the survey by closing the survey web page.

There are no costs for participation in this study. Your participation is voluntary and no payment or compensation will be provided.

Your responses to the survey are anonymous and no personally identifiable information will be collected or stored as part of the research. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. Your privacy will be protected under the General Data protection Regulation (GDPR), as well as under the applicable Canadian and the USA data privacy regulations. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution. All confidential data will be kept securely in an encrypted folder within the system. All data will be kept for 36 months from the end of the study and destroyed after that time through a process of complete deletion from the system.

If you have questions or concerns, you can contact Love James at la969@mynsu.nova.edu or Dr. Ling Wang at lingwang@nova.edu.

If you have questions about the study but prefer to speak with someone else who is not part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at +1(954) 262-5369 or toll free at 1-866-499-0790 or by email at IRB@nova.edu.

If you have read the above information and voluntarily wish to participate in the research study, please click the 'Next' button below to begin the survey.

Privacy embedded Design (PeD)

These questions assess your understanding of the privacy settings associated with the home automation systems.
Please indicate the degree with which you agree to the following statement by ticking a box.

PeD 1: **My home automation system has privacy settings embedded into them.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PeD 2: **I can easily locate the privacy settings on my home automation system.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PeD 3: **The user guide that accompanied my home automation system contains information about privacy settings.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PeD 4: **The user guide for my home automation system provides guidance on how to use the privacy settings of the device.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PeD 5: **The user guide for my home automation system encourages me to change the privacy settings of the device.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Privacy Self-Efficacy (PSE)

These questions assess your ability to use the privacy settings associated with the home automation systems.
Please indicate the degree with which you agree to the following statement ticking only one box.

PSE 1: **I am confident of easily locating the privacy settings of my home automation system.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PSE 2: **I am confident about operating the privacy settings of my home automation system.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PSE 3: **I am confident to select the appropriate privacy settings for my home automation system.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PSE 4: **I understand what the privacy settings of my home automation system represents.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PSE 5: **I understand the privacy setting required to protect the privacy of my home while using the home automation system.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Privacy Concern (PC)

These questions assess your view of the privacy issues associated with the use of home automation systems.

Please indicate the degree with which you agree to the following statement ticking only one box.

PC 1: **I am of the opinion that the use of home automation system creates a privacy concern.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PC 2: **I am of the opinion that the use of home automation system increases the chances of violating the privacy of the home.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PC 3: **I am concerned that using the home automation system will cause the privacy of my home to be invaded.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PC 4: **Including privacy settings in home automation systems will provide privacy assurance.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

PC 5: **Understanding how to use the privacy settings of my home automation system will reduce my privacy concerns.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Home Automation Usage (HAU)

These questions assess your usage of home automation systems.

Please indicate the degree with which you agree to the following statement ticking only one box.

HAU 1: **I currently use or plan to use a home automation system.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

HAU 2: **I will prefer to use a home automation system that has privacy settings included in the device.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

HAU 3: **I will prefer to use a home automation system with a default privacy setting set to protect the privacy of my home.**

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Appendix B

Institutional Review Board Approval

NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Love James**

From: **Wei Li, Ph.D,**
Center Representative, Institutional Review Board

Date: **December 2, 2019**

Re: **IRB #: 2019-562; Title, "Smart Privacy for IoT: Privacy embedded Design for Home Automation Systems"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Wei Li, Ph.D, respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Ling Wang, Ph.D.
Ling Wang, Ph.D.

Appendix C

Output Results for Scale Items Initial Reliability Test

Table C1: *PeD Scale Item Reliability Results*

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.892	.898	5

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PeD_1	6.96	12.685	.583	.441	.910
PeD_2	7.42	12.873	.745	.591	.868
PeD_3	7.27	12.334	.791	.848	.857
PeD_4	7.31	12.436	.792	.870	.857
PeD_5	7.71	12.460	.812	.698	.853

Table C2: *PSE Scale Internal Consistency Reliability Results*

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.939	.943	5

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PSE_1	8.61	20.409	.856	.778	.923
PSE_2	8.74	18.754	.850	.797	.923
PSE_3	8.75	20.055	.878	.852	.919
PSE_4	8.61	18.120	.834	.747	.929
PSE_5	8.68	20.592	.800	.725	.932

Table C3: *PC Scale Internal Consistency Reliability Results*

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.794	.786	5

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PC_1	17.16	8.051	.738	.810	.695
PC_2	17.03	8.110	.756	.847	.687
PC_3	17.39	9.714	.690	.643	.722
PC_4	17.02	11.508	.367	.432	.811
PC_5	17.60	11.480	.353	.436	.816

Table C4a: *HAU Internal Consistency Reliability Results Before Deleting HAU3; HAU4; HAU5*

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.379	.451	6

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
HAU_1	19.01	5.568	.287	.690	.273
HAU_2	18.85	5.909	.400	.592	.259
HAU_3	20.31	5.453	.127	.272	.380
HAU_4	21.13	5.355	.191	.349	.328
HAU_5	20.07	6.029	.068	.164	.411
HAU_6	19.03	5.897	.127	.499	.369

Table C4b: *HAU Internal Consistency Reliability Results After Deleting HAU3; HAU4; HAU5*

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.804	.830	3

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
HAU_1	9.48	1.642	.771	.664	.598
HAU_2	9.32	2.389	.683	.586	.755
HAU_3	9.50	1.642	.593	.375	.835

Table C5: *Scale Internal Consistency Reliability Results for All the Scale Items*

Reliability Statistics

Cronbach's Alpha	N of Items
.751	17

Item-Total Statistics

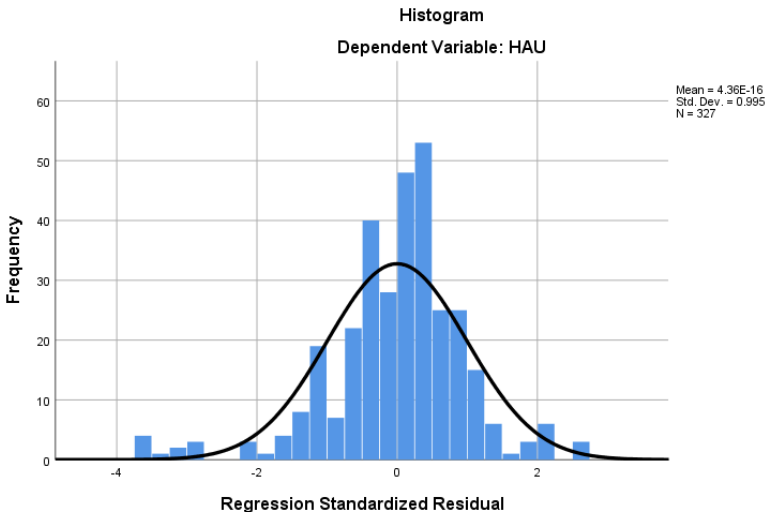
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
PeD_1	50.89	61.152	.292	.744
PeD_2	51.30	58.813	.510	.724
PeD_3	51.12	61.855	.269	.746
PeD_4	51.21	61.853	.284	.744
PeD_5	51.60	58.946	.548	.722
PSE_1	50.88	54.288	.729	.701
PSE_2	51.04	53.101	.692	.700
PSE_3	50.96	54.928	.701	.704
PSE_4	50.92	53.533	.607	.709
PSE_5	50.98	57.006	.503	.722
PC_1	48.90	64.413	.201	.749
PC_2	48.73	66.715	.070	.757
PC_4	49.06	68.131	-.051	.767
PC_5	49.44	66.202	.068	.760
HAU_1	49.03	67.012	.016	.763
HAU_2	48.80	66.006	.124	.753
HAU_3	48.84	69.216	-.121	.772

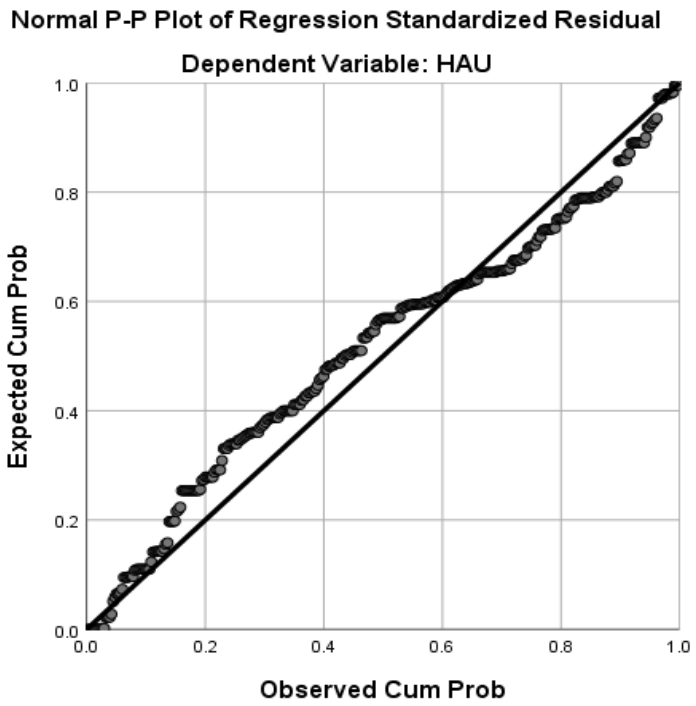
Appendix D

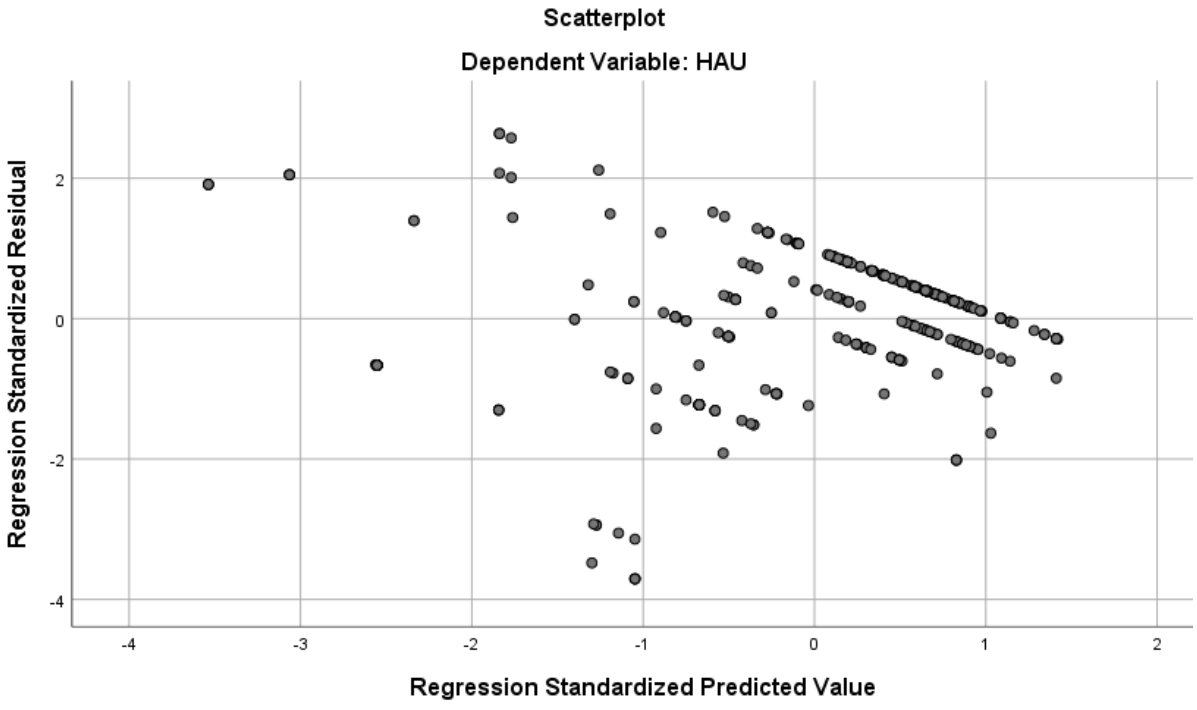
Descriptive Statistics and Test of Normality Output Results

Descriptives

			Statistic	Std. Error
MAH_3	Mean		2.8469109	.16957512
	95% Confidence Interval for Mean	Lower Bound	2.5132555	
		Upper Bound	3.1805664	
	5% Trimmed Mean		2.5752400	
	Median		1.3861607	
	Variance		9.001	
	Std. Deviation		3.00009016	
	Minimum		.15697	
	Maximum		11.91260	
	Range		11.75563	
	Interquartile Range		2.55320	
	Skewness		1.431	.138
	Kurtosis		.593	.275

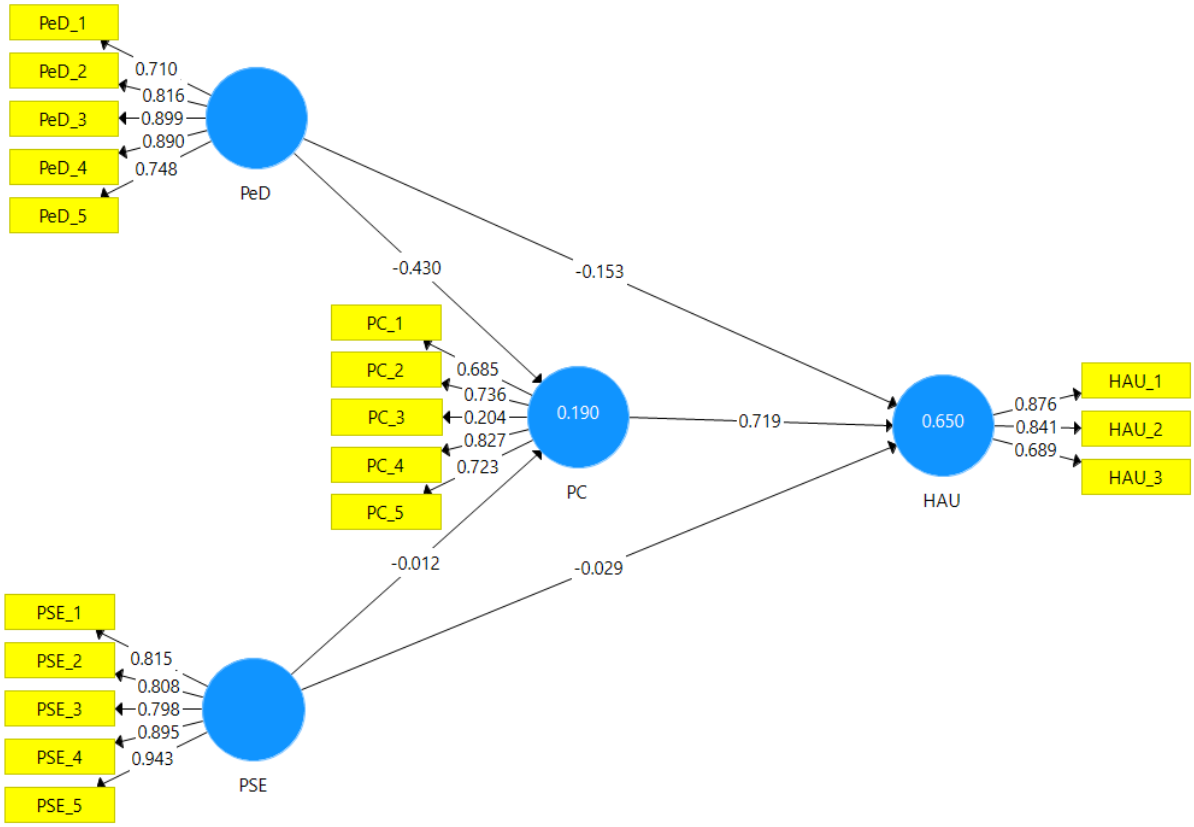



Normal P-P Plot of Regression Standardized Residual
Dependent Variable: HAU
Expected Cum Prob
Observed Cum Prob
0.0
0.2
0.4
0.6
0.8
1.0


Scatterplot
Dependent Variable: HAU
Regression Standardized Residual
Regression Standardized Predicted Value
2
0
-2
-4
-3
-1
1

APPENDIX E

Initial SmartPLS Output Results for Factor Loadings



Appendix F

Initial SmartPLS Output Results for Model fit, Reliability, Validity and Outer Loadings

Model Fit

Fit Summary

	Saturated Model	Estimated Model
SRMR	0.117	0.117
d_ULS	2.336	2.336
d_G	0.907	0.907
Chi-Square	1611.448	1611.448
NFI	0.609	0.609

Construct Reliability and Validity

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
HAU	0.726	0.746	0.846	0.650
PC	0.693	0.774	0.786	0.452
PSE	0.927	1.347	0.930	0.729
PeD	0.878	0.945	0.908	0.666

Discriminant Validity

Fornell-Larcker Criterion

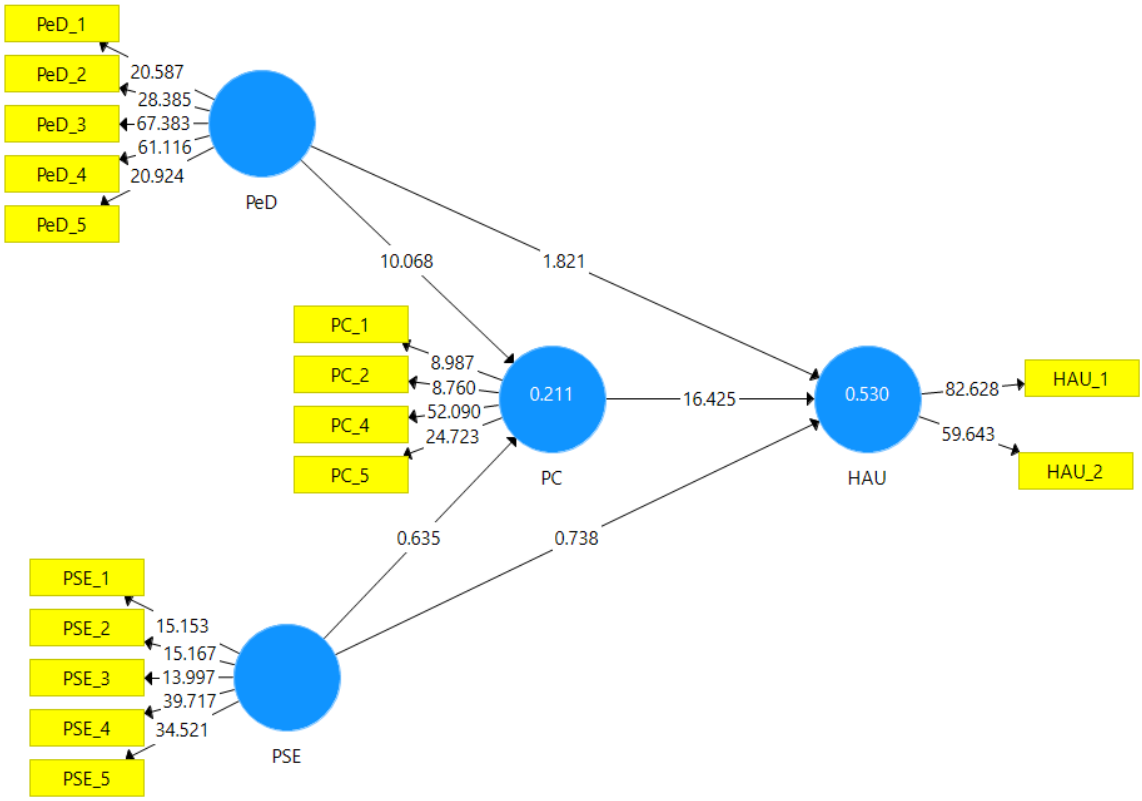
	HAU	PC	PSE	PeD
HAU	0.806			
PC	0.792	0.672		
PSE	-0.240	-0.200	0.854	
PeD	-0.479	-0.436	0.437	0.816

Outer Loadings

	HAU	PC	PSE	PeD
HAU_1	0.876			
HAU_2	0.841			
HAU_3	0.689			
PC_1		0.685		
PC_2		0.736		
PC_3		0.204		
PC_4		0.827		
PC_5		0.723		
PSE_1			0.815	
PSE_2			0.808	
PSE_3			0.798	
PSE_4			0.895	
PSE_5			0.943	
PeD_1				0.710
PeD_2				0.816
PeD_3				0.899
PeD_4				0.890
PeD_5				0.748

Appendix G

Final SmartPLS Output Results for Factor Loadings after deleting HAU3 and PC3



APPENDIX H

Final SmartPLS Output Results for Model fit, Reliability, Validity

Model Fit

Fit Summary

	Saturated Model	Estimated Model
SRMR	0.051	0.051
d_ULS	0.354	0.350
d_G	0.210	0.210
Chi-Square	1694.881	1694.881
NFI	0.981	0.981

Construct Reliability and Validity

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
HAU	0.816	0.816	0.916	0.845
PC	0.746	0.818	0.831	0.553
PSE	0.930	1.358	0.935	0.744
PeD	0.889	0.938	0.916	0.687

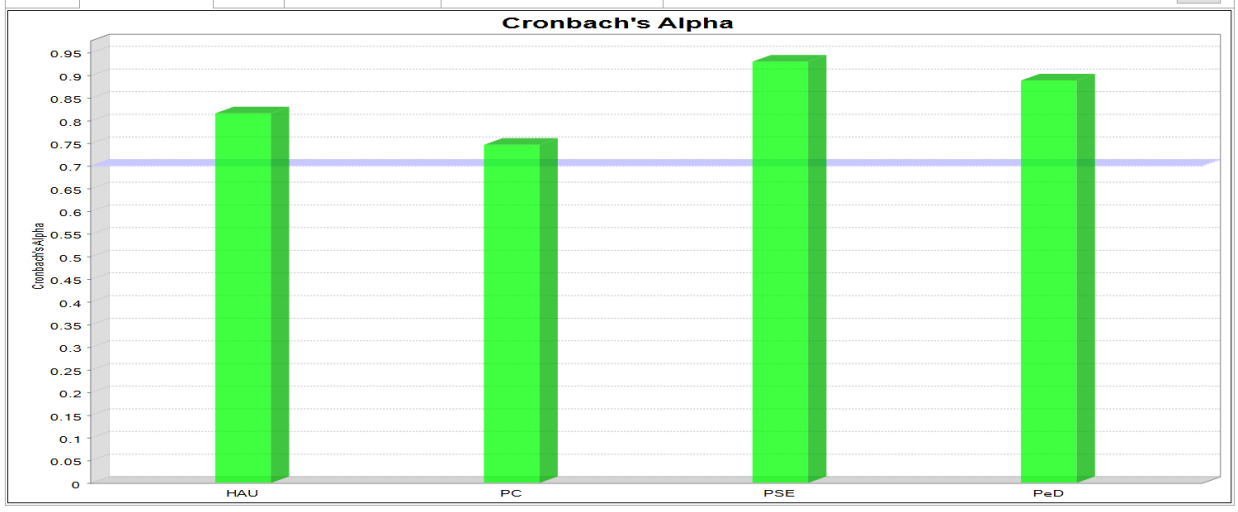
Discriminant Validity

Fornell-Larcker Criterion

	HAU	PC	PSE	PeD
HAU	0.**919**			
PC	0.724	**0.744**		
PSE	-0.208	-0.227	**0.863**	
PeD	-0.394	-0.459	0.454	**0.829**

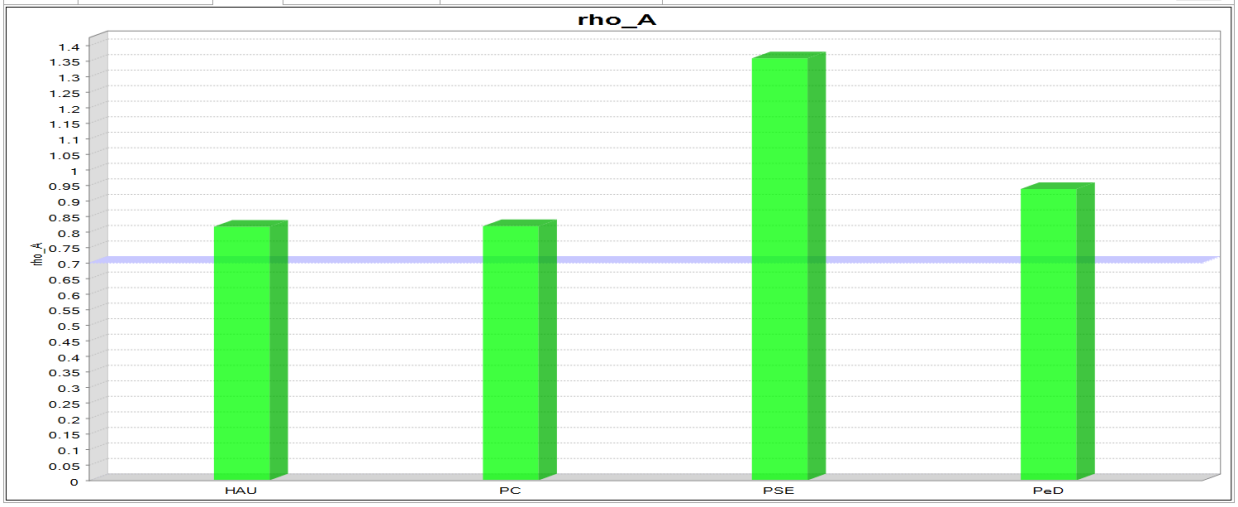
Construct Reliability and Validity

Matrix | Cronbach's Alpha | rho_A | Composite Reliability | Average Variance Extracted (AVE) | Copy to Clipboard: Chart



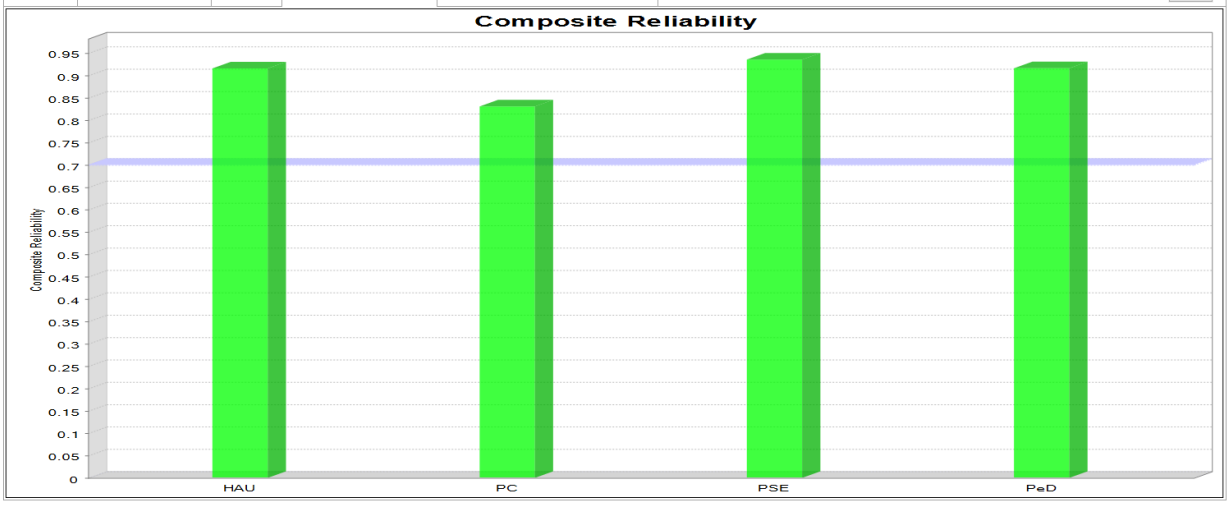
Construct Reliability and Validity

Matrix | Cronbach's Alpha | rho_A | Composite Reliability | Average Variance Extracted (AVE) | Copy to Clipboard: Chart



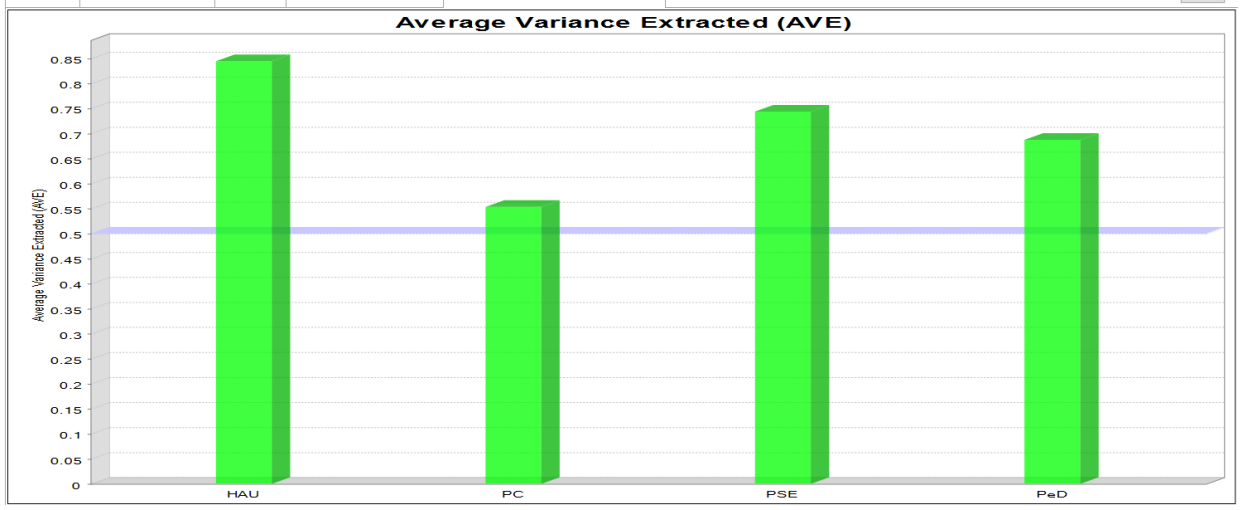
Construct Reliability and Validity

Matrix | Cronbach's Alpha | rho_A | Composite Reliability | Average Variance Extracted (AVE) | Copy to Clipboard: Chart



Construct Reliability and Validity

Matrix | Cronbach's Alpha | rho_A | Composite Reliability | Average Variance Extracted (AVE) | Copy to Clipboard: Chart



Final SmartPLS Output Results for Outer Loadings after deleting HAU3 and PC3

Outer Loadings

	HAU	PC	PSE	PeD
HAU_1	0.922			
HAU_2	0.916			
PC_1		0.660		
PC_2		0.681		
PC_4		0.853		
PC_5		0.765		
PSE_1			0.838	
PSE_2			0.822	
PSE_3			0.826	
PSE_4			0.885	
PSE_5			0.936	
PeD_1				0.719
PeD_2				0.817
PeD_3				0.898
PeD_4				0.898
PeD_5				0.801

Appendix I

PROCESS macro Output Results for Mediation Tests

```
Model  : 4
    Y  : HAU
    X  : PeD
    M  : PC
Sample
Size:  313
**************************************************************************
OUTCOME VARIABLE:
 PC
Model Summary
  R      R-sq     MSE       F          df1        df2          p
.3908   .1527    7.3423    56.0655     1.0000   311.0000   .0000
Model
          coeff     se      t          p    LLCI     ULCI
constant 19.7820   .3779  52.3413  .0000  19.0384  20.5257
PeD       -.2450   .0327  -7.4877  .0000   -.3094   -.1806 ← Path a
**************************************************************************
OUTCOME VARIABLE:
 HAU
Model Summary
  R       R-sq    MSE       F       df1        df2           p
.6788    .4607   1.4328  132.4276   2.0000   310.0000    .0000
Model
          coeff     se       t         p     LLCI      ULCI
constant 3.5951   .5229   6.8752    .0000   2.5662  4.6240
PeD      -.0458   .0157  -2.9173    .0038   -.0767  -.0149 ← Path c'
PC        .3406   .0250  13.5973    .0000    .2913   .3899 ← Path b
*********************** TOTAL EFFECT MODEL ****************************
OUTCOME VARIABLE:
 HAU
Model Summary
    R      R-sq      MSE         F      df1        df2          p
 .3730    .1391   2.2801   50.2550   1.0000   311.0000      .0000
Model
          coeff       se        t        p     LLCI   ULCI
constant  10.3330   .2106   49.0619   .0000   9.9186  10.7474
PeD       -.1293    .0182   -7.0891   .0000   -.1651   -.0934 ← Path c
************ TOTAL, DIRECT, AND INDIRECT EFFECTS OF X ON Y ************
Total effect of X on Y
  Effect        se        t        p     LLCI    ULCI
  -.1293     .0182   -7.0891   .0000   -.1651   -.0934 ← Path c
Direct effect of X on Y
  Effect      se       t        p    LLCI    ULCI
  -.0458   .0157  -2.9173   .0038  -.0767   -.0149 ← Path c'
Indirect effect(s) of X on Y:
       Effect     BootSE   BootLLCI   BootULCI
PC     -.0835      .0183     -.1241     -.0508 ←  ab with 95% bootstrap confidence interval

******** ANALYSIS NOTES AND ERRORS***************
Level of confidence for all confidence intervals in output:   95.0000

Number of bootstrap samples for percentile bootstrap confidence
intervals:   5000

------ END MATRIX -----
```

```
Model  : 4
    Y  : HAU
    X  : PSE
    M  : PC

Sample
Size:  313
**************************************************************************
OUTCOME VARIABLE:
 PC
Model Summary
 R      R-sq    MSE      F      df1        df2        p
.1236  .0153   8.5337  4.8211  1.0000   311.0000  .0289
Model
           coeff      se        t       p      LLCI     ULCI
constant 17.9725   .3908  45.9935   .0000   17.2036  18.7414
PSE       -.0649   .0296  -2.1957   .0289    -.1230   -.0067  <-- Path a
**************************************************************************
OUTCOME VARIABLE:
 HAU
Model Summary
   R     R-sq     MSE      F       df1       df2          p
.6705   .4495   1.4626  126.5813  2.0000   310.0000   .0000
Model
           coeff      se     t      p     LLCI     ULCI
constant  2.9020   .4519   6.4222  .0000  2.0128  3.7911
PSE       -.0176   .0123  -1.4254  .1550  -.0418  .0067  <--Path c'
PC         .3650   .0235  15.5496  .0000   .3188  .4112  <--Path b

*********************** TOTAL EFFECT MODEL ****************************
OUTCOME VARIABLE:
 HAU
Model Summary
 R       R-sq    MSE       F      df1       df2          p
.1421  .0202    2.5950  6.4103   1.0000   311.0000   .0118
Model
          coeff     se      t         p    LLCI    ULCI
constant 9.4625  .2155  43.9130  .0000   9.0385  9.8865
PSE      -.0413  .0163  -2.5319  .0118   -.0733  -.0092  <--Path c

*********** TOTAL, DIRECT, AND INDIRECT EFFECTS OF X ON Y ***********
Total effect of X on Y
Effect    se      t          p    LLCI     ULCI
-.0413  .0163   -2.5319  .0118  -.0733   -.0092  <-- Path c
Direct effect of X on Y
Effect       se      t           p     LLCI    ULCI
-.0176    .0123    -1.4254   .1550    -.0418  .0067  <-- Path c'
Indirect effect(s) of X on Y:
       Effect     BootSE   BootLLCI   BootULCI
PC     -.0237      .0089     -.0418     -.0072  <--  ab with 95% bootstrap
                                                    confidence interval

******** ANALYSIS NOTES AND ERRORS***************
Level of confidence for all confidence intervals in output:   95.0000

Number of bootstrap samples for percentile bootstrap confidence
intervals:   5000

------ END MATRIX -----
```

Appendix J

Post-hoc Power Analysis Output Results

Post-hoc Statistical Power Calculator for Multiple Regression

This calculator will tell you the observed power for your multiple regression study, given the observed probability level, the number of predictors, the observed R^2, and the sample size.

Please enter the necessary parameter values, and then click 'Calculate'.

Number of predictors: 2
Observed R^2: 0.530
Probability level: 0.05
Sample size: 313
Calculate!

Observed statistical power: 1.0

Post-hoc Statistical Power Calculator for Multiple Regression

This calculator will tell you the observed power for your multiple regression study, given the observed probability level, the number of predictors, the observed R^2, and the sample size.

Please enter the necessary parameter values, and then click 'Calculate'.

Number of predictors: 3
Observed R^2: 0.53
Probability level: 0.05
Sample size: 313
Calculate!

Observed statistical power: 1.0

References

Abdulrahman, T. A., Isiwekpeni, O. H., Surajudeen-Bakinde, N. T., & Otuoze, A. O. (2016). Design, specification and implementation of a distributed home automation system. *Procedia Computer Science, 94*, 473-478.

Abomhara, M., & Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. *Privacy and Security in Mobile Systems (PRISMS), pp. 1-8*. IEEE.

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. *Proceedings of the 1st ACM Conference on Electronic Commerce, pp. 1-8.* ACM.

Acquisti, A., and Grossklags, J. (2003), Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. *Proceedings of the 2nd Annual Workshop on Economics and Information Security* (WEIS 2003), May 29-30, 2003, Maryland, USA.

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic commerce, pp. 21-29*. ACM.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy, 3(1),* 26-33.

Acquisti, A., and Grossklags, J. (2007), What can behavioral economics teach us about privacy. *Digital Privacy: Theory, Technology, and Practices, 18, 363-377.*

Ajzen, I. (1988). From intentions to action. *Attitudes, Personality, and Behavior*, 112-145.

Ajzen, I., & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. Eaglewood Cliffs, NJ: Prentice-Hall.

Alam, M. R., Reaz, M. B. I., & Ali, M. A. M. (2012). A review of smart homes—Past, present, and future. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 42*(6*),* 1190-1203.

Aloudat, A., & Michael, K. (2011). Toward the regulation of ubiquitous mobile government: A case study on location-based emergency services in Australia. *Electronic Commerce Research, 11(1),* 31-74.

Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed embedded security framework for internet of things (IoT). *Proceedings of the 2nd*

International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronics Systems Technology (Wireless VITAE) pp. 1-5. IEEE.

Baek, Y. M. (2014). Solving the privacy paradox: A counter-argument experimental approach. *Computers in human behavior*, *38*, 33-42.

Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. *Administrative Science Quarterly*, *36*, 421-458.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, *84*(2), 191.

Bandura, A. (1986). The explanatory and predictive scope of self-efficacy theory. *Journal of Social and Clinical Psychology*, *4*(3), 359-373.

Barney, J. B., & Hansen, M. H. (1994). Trustworthiness as a source of competitive advantage. *Strategic Management Journal*, *15*(S1), 175-190.

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

Bentler, P.M. & Bonnet, D.C. (1980), Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin*, 88 (3), 588-606.

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

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. Textbooks Collection 3. Available at: http://scholarcommons.usf.edu/oa_textbooks/3. Accessed on: September 12, 2017.

Boneh, D., Lynn, B., & Shacham, H. (2004). Short signatures from the weil pairing. *Journal of Cryptology*, *17(4)*, 297-319.

Borena, B., Belanger, F., & Ejigu, D. (2013). Social networks and information privacy: A model for low-income countries. *Proceedings of the 19th Americas Conference on Information Systems (AMCIS). Chicago, Illinois, August 15-17, 2013*.

Borking, J. J., & Raab, C. D. (2001). Laws, PETs, and other technologies for privacy protection. *Journal of Information, Law and Technology*, *1*, 1-14.

Brown, J. S. (2001). Knowledge and organization: A social-practice perspective. *Organization Science* 12: 198–213.

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.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy and Marketing*, *19*(1*)*, 7-19.

Cavoukian, A. (2012). Privacy by design. *IEEE Technology and Society Magazine, 31(4),* 18-19.

Cavoukian, A., & Tapscott, D. (1996). *Who Knows: Safeguarding Your Privacy in a Networked World.* McGraw-Hill Professional.

Chapple, M., Stewart, J. M., & Gibson, D. (2018). *(ISC)^2 Certified Information Systems Security Professional (CISSP). Official Study Guide*. John Wiley and Sons.

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

Cho, H. (2010). Determinants of behavioral responses to online privacy : The effects of concern, risk beliefs, self-efficacy, and communication sources on self-protection strategies. *Journal of Information Privacy and Security, 6(1), 3–27.*

Clarke, R., Daly, L., Robinson, K., Naughten, E., Cahalane, S., Fowler, B., & Graham, I. (1991). Hyperhomocysteinemia: An independent risk factor for vascular disease. *New England Journal of Medicine, 324(17),* 1149-1155.

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155.

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

Covington, M. J., & Carskadden, R. (2013). Threat implications of the internet of things. *Proceedings of the 5th International Conference on In Cyber Conflict (CyCon), pp. 1-12.* IEEE.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104-115.

Culnan, M. J, & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59(2),* 323-342.

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

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10(2),* 7-29.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17(1),* 61-80.

Dinev, T., McConnell, R. A., Smith, H. J. (2015). Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research, 26(4),* 639-655.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. European *Journal of Information Systems, 22(3),* 295–316.

D'Souza, G., and Phelps, J. E. (2009), The privacy paradox: The case of secondary disclosure. *Review of Marketing Science*, 7(1).

Federal Trade Commission. (2014). Analysis of proposed consent order to aid public comment marketer of internet-connected home security video cameras. Washington, USA: Federal Trade Commission.

Federal Trade Commission (2000). Privacy online: Fair information practices in the electronic marketplace, a report to congress, Washington DC, available online at: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [accessed: 20 January 2020].

Fensel, A., Kumar, V., & Tomic, S. D. K. (2014). End-user interfaces for energy-efficient semantically enabled smart homes. *Energy Efficiency*, *7(4),* 655-675.

Field, A.P. (2018). *Discovering Statistics Using IBM SPSS Statistics* (North American ed.). London: Sage.

Fornell, C. and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18 (1), 39–50.

Ganesan, S. (1994). Determinants of long-term orientation in buyer seller relationships. *Journal of Marketing Research* 58, 1-19.

Gay, L. R., Mills, G. E., & Airasian, P. W. (2009). *Educational Research: Competencies for Analysis and Applications*. Merrill: Pearson.

Growth from Knowledge. (2016). Smart home: the truth behind the hype. http://www.gfk.com/landing-pages/smart-home-white-paper/.

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

Hair, F., H., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (Second Ed.). Thousand Oaks: SAGE Publications, Inc.

Han, M., Li, L., Xie, Y., Wang, J., Duan, Z., Li, J., & Yan, M. (2018). Cognitive approach for location privacy protection. *IEEE Access*, *6*, 13466-13477.

Hann, I.H., Hui, K.L., Lee, S.Y.T., and Png, I. P. (2007), Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, 24(2), 13-42.

Hasan, B. (2006). Delineating the effects of general and system-specific computer self-efficacy beliefs on IS acceptance. *Information and Management*, *43*(5), 565-571.

Hayes, A. F. (2012). PROCESS: A versatile computational tool for observed variable mediation, moderation, and conditional process modeling. Retrieved from: http://www.afhayes.com/public/process2012.pdf.

Hayes, A. F., & Rockwood, N. J., (2016). Regression-based statistical mediation and moderation analysis in clinical research: Observations, recommendations, and implementation. *Behavior Research and Therapy.* 1, 1-19.

Hayes, A. F. (2017). *Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*. Guilford publications.

Hayes, A. F., Montoya, A. K., & Rockwood, N. J. (2017). The analysis of mechanisms and their contingencies: PROCESS versus structural equation modeling. *Australasian Marketing Journal*, 25, 76–81.

Hernandez, G., Arias, O., Buentello, D., & Jin, Y. (2014). Smart nest thermostat: A smart spy in your home. Black Hat, USA.

Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers and Security*, 53, 1-17.

Hjorth, T. S., & Torbensen, R. (2012). Trusted Domain: A security platform for home automation. *Computers and Security*, 31(8), 940-955.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal*, *20*(2), 195-204.

Hu, L.T. and Bentler, P.M. (1999), Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling*, 6 (1), 1-55.

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719-733.

Jacobsson, A., & Davidsson, P. (2015). Towards a model of privacy and security for smart homes. *Proceedings of the 2nd World Forum on Internet of Things (WF-IoT)*, pp. 727-732. IEEE.

James, L. R., Mulaik, S. A., & Brett, J. M. (1982). *Causal Analysis: Assumptions, Models, and Data*. Beverly Hills, CA: Sage.

Johnston, A., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549–566.

Kaldestad, Ø. H. (2016). Fitness wristbands violate European law. (Forbrukerråde). Available in: https://www.forbrukerradet.no/side/fitness-wristbands-violate-european-law/. Retrieved on: September 17, 2017.

Kalofonos, D. N., & Shakhshir, S. (2007). Intuisec: a framework for intuitive user interaction with smart home security using mobile devices. *Proceedings of the IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1-5. IEEE.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. (2015). The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, *25*(6), 637-667.

Keith, M. J., Babb, J., Furner, C., Abdullat, A., & Lowry, P. B. (2016). Limited information and quick decisions: consumer privacy calculus for mobile applications. *AIS Transactions on Human-Computer Interaction (THCI)*, *8*(3), 88-130.

Kennedy, J. J., & Bush, A. J. (1985). An Introduction to the Design and Analysis of Experiments in Behavioral Research. University Press of America.

Kline, P. (1999). *The Handbook of Psychological Testing* (2nd ed.). London: Routledge.

Kong, N. (2008). Research on key technology of the resource addressing in the internet of things. *Computer Network Information Center, Chinese Academy of Sciences*, 33-68. Beijing.

Koreshoff, T. L., Robertson, T., & Leong, T. W. (2013). Internet of things: a review of literature and products. *Proceedings of the 25th Australian Computer-Human*

Interaction Conference: Application, Innovation, Collaboration, pp. 335-344. ACM.

Kramp, T., Van Kranenburg, R., & Lange, S. (2013). *Enabling Things to Talk*. Springer, Berlin, Heidelberg.

Kriaa, S., Bouissou, M., & Pièrre-Cambacédès, L. (2012). Modeling the Stuxnet attack with BDMP: Towards more formal risk assessments. *Proceedings of* the *7th International Conference on Risk and Security of Internet and Systems (CRiSIS)*, pp. 1-8. IEEE.

Kozlov, D., Veijalainen, J., & Ali, Y. (2012). Security and privacy threats in IoT architectures. *Proceedings of the 7th International Conference on Body Area Networks*, pp. 256-262. Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST).

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers and Security*, *64*, 122-134.

Lai, M. L. (2008). Technology readiness, internet self-efficacy and computing experience of professional accounting students. *Campus-Wide Information Systems*, *25*(1), 18-29.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE, Security and Privacy*, 9(3), 49-51.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, 33(3), 22-42.

Lee, C., Zappaterra, L., Choi, K., & Choi, H. A. (2014). Securing smart home: Technologies, security challenges, and security requirements. *Proceedings of the 2014 Conference on Communications and Network Security*, pp. 67-72. IEEE.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, 51(3), 434-445.

Li, Y. (2014). A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications*, *13*(1), 32-44.

Lin, H., Bergmann, N.W. (2016). IoT privacy and security challenges for smart home *Environments. Information*, 7(44), 1-15.

Losilla, F., Vicente-Chicote, C., Álvarez, B., Iborra, A., & Sánchez, P. (2007). Wireless sensor network application development: An architecture-centric mode approach. *Proceedings of the 2007 European Conference on Software Architecture*, pp. 179-194. Berlin Heidelberg: Springer.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, *27*(4), 163-200.

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication*, *57*(2), 123-146.

Lu, Y., Tan, B., and Hui, K.-L. 2004. Inducing Customers to disclose personal information to internet businesses with social adjustment benefits. *Proceedings of the 25th International Conference on Information Systems*, pp. 272-281. Washington, DC.

Lutolf, R. (1992, November). Smart home concept and the integration of energy meters into a home-based system. *Proceedings of the 7th International Conference on Metering Apparatus and Tariffs for Electricity Supply 1992*, pp. 277-278. IET.

MacKinnon, D. P., Fairchild, A. J., & Fritz, M. S. (2007). Mediation analysis. *Annual Review of Psychology*, *58*, 593-614.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, 5-12.

McCarthy, J. T. (1986). Melville B. Nimmer and the Right of Publicity: A tribute. *Ucla Law Review*, 34, 1703.

McDonald, T., & Siegall, M. (1992). The effects of technological self-efficacy and job focus on job performance, attitudes, and withdrawal behaviors. *The Journal of Psychology*, 126(5), 465-475.

MacKinnon, D. P., & Dwyer, J. H. (1993). Estimating mediated effects in prevention studies. *Evaluation Review*, *17*(2), 144-158.

MacKinnon, D. P., Coxe, S., & Baraldi, A. N. (2012). Guidelines for the investigation of mediating variables in business research. *Journal of Business and Psychology*, *27*(1), 1-14.

MacKinnon, D. P., & Pirlott, A. G. (2015). Statistical approaches for enhancing causal interpretation of the M to Y relation in mediation analysis. *Personality and Social Psychology Review*, *19*(1), 30-43.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The journal of Strategic Information Systems*, *11*(3-4), 297-323.

Mertler, C.A., & Vannatta, R.A. (2013). *Advanced and Multivariate Statistical Methods: Practical Application and Interpretation* (3rd ed.). Los Angeles, CA: Pyrczak Publishing.

Milberg, S. J., Smith, H. J., and Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, 11(1), 35-57.

Muthén, L. K., & Muthén, B. O. (2002). How to use a Monte Carlo study to decide on sample size and determine power. *Structural Equation Modeling*, *9*(4), 599-620

Myrstad, F. (2016). Connected toys violate European consumer law. (Forbrukerråde). Available in: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/. Retrieved on: September 18, 2017.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126.

Ormond, D., Warkentin, M., Johnston, A. C., & Thompson, S. C. (2016). Perceived deception: Evaluating source credibility and self-efficacy. *Journal of Information Privacy and Security*, *12*(4), 197-217.

Parent, W. A. (1983). Recent work on the concept of privacy. *American Philosophical Quarterly*, *20*(4), 341-355.

Pedersen, D. M. (1999). "Model for Types of Privacy by Privacy Functions. *Journal of Environmental Psychology*, 19(4), 397-405.

Peppet, S. R. (2014). Regulating the Internet of things: First steps towards managing discrimination, privacy, security, and consent. *Texas Law Review*, 93,85–176.

Peter, J. P., & Tarpey, L. X. (1975). A comparative analysis of three consumer decision strategies. *Journal of Consumer Research*, 2(1), 29-37.

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

Pishva, D. (2017). Internet of Things: Security and privacy issues and possible solution. *Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT)*, pp. 797-808. IEEE.

Pishva, D. (2017). IoT: Their conveniences, security challenges and possible solutions. *Advanced Science Technology Engineering System Journal*, *2*(3), 1211-1217.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities. *European Journal of Information Systems*, *19*(2), 181-195.

Powers, M. (1996). A cognitive access definition of privacy. *Law and Philosophy, 15(4),* 369-386.

Rea, L. M., & Parker, R. A. (2014). *Designing and Conducting Survey Research: A Comprehensive Guide*. John Wiley and Sons.

Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy,* Chapel Hill: NC University of North Carolina Press.

Riahi, A., Natalizio, E., Challal, Y., Mitton, N., & Iera, A. (2014). A systemic and cognitive approach for IoT security. *Proceedings of the 2014 International Conference on Computing, Networking and Communications (ICNC)*, pp. 183-188. IEEE.

Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Delahoche, L., & Loge, C. (2006). The smart home concept: Our immediate future. *Proceedings of the 1st IEEE international Conference on E-learning in Industrial Electronics*, pp. 23-28. IEEE.

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs*, *39*(2), 339-362.

Sadeghi, A., Wachsmann, C., Waidner, M. (2015). Security and Privacy Challenges in Industrial Internet of Things. *Proceedings of the 52nd Design Automation Conference (DAC)*, pp. 1-6. ACM/EDAC/IEEE.

Saunders, M., Lewis, P., and Thornhill, A., 2016. *Research Methods for Business Students*. 7th ed. Pearson Education Limited, England.

Segars, A. H., & Grover, V. (1993). Re-examining perceived ease of use and usefulness: A confirmatory factor analysis. *MIS Qarterly*, 17(4), 517-525.

Sekaran, U., & Bougie, R. (2013). *Research Methods for Business*. John Wiley and Sons.

Selten, R. (1999). 'What is bounded rationality? *Marketing Letters* 10(3), 233-248. Springer, The Netherlands.

Sheehan, K. B. (2002). Toward a typology of internet users and online privacy concerns. *Information Society*, 18(1), 21-32.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy, and trust in internet of things: The road ahead. *Computer Networks*, *76*, 146-164.

Simon, H. A. (1972). Theories of bounded rationality. *Decision and Organization*, *1*(1), 161-176.

Simon, H. A. (1997). *Models of bounded rationality: Empirically Grounded Economic Reason* (Vol. 3). MIT Press.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, 35(4), 989-1016.

Soper, D., (2020). Post-hoc online statistical Power Calculator, available at: https://www.danielsoper.com/statcalc/calculator.aspx?id=9.

Spiekermann, S. (2012). The challenges of privacy by design. *Communications of the ACM*, *55*(7), 38-40.

Stone-Romero, E.F. & Rosopa, P. (2004). Inference problems with hierarchical multiple regression-based tests of mediating effects. *Research in Personnel and Human Resources Management* 23, 249-290. Greenwich, CT: Elsevier.

Sun, G., Huang, S., Bao, W., Yang, Y., & Wang, Z. (2014). A privacy protection policy combined with privacy homomorphism in the internet of things. *Proceedings of the 2014 International Conference on Computer Communication and Networks* (ICCCN), pp. 1-6. IEEE.

Tabachnick, B. G., & Fidell, L. S. (1996). *Using Multivariate Statistics*. Northridge: Harper Collins.

Taylor, A. B., MacKinnon, D. P., & Tein, J. Y. (2008). Tests of the three-path mediated effect. *Organizational Research Methods*, *11*(2), 241-269.

Thomas, K. W., & Velthouse, B. A. (1990). Cognitive elements of empowerment: An "interpretive" model of intrinsic task motivation. *Academy of management review*, *15*(4), 666-681.

Tsai, J. Y., Egelman, S., Cranor, L. and Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2), 254-268.

Tozlu, S., Senel, M., Mao, W., & Keshavarzian, A. (2012). Wi-Fi enabled sensors for internet of things: A practical approach. *IEEE Communications Magazine*, *50*(6), 134-143.

Tukey, J. W. (1980). *Styles of Data Analysis, and their Implications for Statistical Computing*. New Jersey: Princeton University Press.

Van Dyke, T. P., Midha, V., & Nemati, H. (2007). The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. *Electronic Markets*, *17*(1), 68-81.

Van Eerde, W., & Thierry, H. (1996). Vroom's expectancy models and work-related criteria: A meta-analysis. *Journal of Applied Psychology*, 81(5), 575.

VanVoorhis, C. W., & Morgan, B. L. (2007). Understanding power and rules of thumb for determining sample sizes. *Quantitative Methods for Psychology*, *3*(2), 43-50.

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

Venkatesh, V., Speier, C., & Morris, M. G. (2002). User acceptance enablers in individual decision making about technology: Toward an integrated model. *Decision Sciences*, *33*(2), 297-316.

Verhulst, B., Eaves, L. J., & Hatemi, P. K. (2012). Correlation not causation: The relationship between personality traits and political ideologies. *American Journal of Political Science*, *56*(1), 34-51.

Vijayasarathy, L. R. (2004). Predicting consumer intentions to use on-line shopping: The case for an augmented technology acceptance model. *Information and Management*, 41(6), 747–762.

Vroom, V.H. (1964). *Work and Motivation*. New York: Wiley.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems*, *22*(2), 157-174.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 193-220.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law and Security Review*, 26(1), 23-30.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.

Wilson, D. W., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. *Proceedings of the 33rd International Conference on Information Systems, ICIS 2012*, pp. 4152-4162. Orlando, Florida USA.

Wood, R. E., Goodman, J. S., Beckmann, N., & Cook, A. (2008). Mediation testing in management research: A review and proposals. *Organizational Research Methods*, *11*(2), 270-295.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 1.

Xu, H., Teo, H. H., & Tan, B. (2005). Predicting the adoption of location-based services: the role of trust and perceived privacy risk. *Proceedings of the 26th International Conference on Information Systems*(ICIS), pp. 1-15. Las Vegas.

Yang, H. L., & Miao, X. M. (2008). Concern for information privacy and intention to transact online. *Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4. IEEE.

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.

Yzer, M. (2017). Theory of reasoned action and theory of planned behavior. *The International Encyclopedia of Media Effects*, 1-7.