Summer 2018

The effects of privacy violation abstractness on privacy attitudes and behaviors

Delicia Anceisao Vaz

THE EFFECTS OF PRIVACY VIOLATION ABSTRACTNESS ON PRIVACY ATTITUDES AND BEHAVIORS

by

DELICIA ANCEISAO VAZ

A THESIS

Presented to the Faculty of the Graduate school of

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE IN INDUSTRIAL-ORGANIZATIONAL PSYCHOLOGY

2018

Approved by:

Denise A. Baker, Advisor
Clair Reynolds Kueny
Susan Murray

ABSTRACT

This research investigates new methods to present privacy policy information to consumers. It makes the argument that current privacy policies do not present consumers with information in a manner that helps align their privacy attitudes with their privacy behaviors. With the introduction of smart appliances to the market, it is critical that appropriate privacy policies are created to equip consumers with information that is easy to understand. Neutral Examples and Risk Examples were created along with the Traditional Content of a privacy policy. These three components were used in different combinations to provide privacy information about smart appliances. Additionally, it was argued that technology literacy of the consumers might affect alignment of privacy attitudes and behaviors. New scales were developed to measure privacy behaviors and technology literacy, and privacy attitudes scales were developed using existing measures as a guide. Moderated mediation analyses revealed that an interaction between Hardware Technology Literacy and certain component combinations (less abstract privacy policies) influenced privacy behaviors, by influencing privacy attitudes. It also revealed that certain privacy attitudes mediated the effect of less abstract privacy policies on privacy behaviors. Additionally, less abstract privacy policies directly influenced privacy behaviors when technology literacy was high. The study concludes that less abstract privacy policies, where Neutral Examples are combined with Traditional Content or Risk Examples, and high technology literacy help improve the consistency between privacy attitudes and behaviors.

Keywords: privacy policy, privacy examples, privacy attitudes, privacy behaviors, technology literacy.

ACKNOWLEDGEMENTS

I express my sincere gratitude towards my advisor, Dr. Denise A. Baker for her guidance and support during my entire time here in this program. Her ability to think outside the box, as well as her patience, and encouragement have made this thesis project possible. I would also like to thank Dr. Clair Reynolds Kueny for her unending supply of motivation and statistical expertise. Her ability to clearly explain complex concepts helped me tackle an analysis of this magnitude. I also thank Dr. Susan Murray for her time, encouragement, and problem solving abilities that enabled me to stay on track and cross the finish line. Without my committee, this project would not have been possible. Together, they have helped me become a better researcher.

To all my friends at Missouri S&T and across the world, thank you. My friends, Shannen, Sozan, and Stephanie, get a special mention for the support they have given me over the years. Thank you for being some of my biggest sources of encouragement.

I am incredibly grateful for the support of my family. I thank my brothers who, in their own ways, helped me walk this path. I especially thank my younger brother, Darwin, for hearing out my ideas, being up for adventures, never letting me down, and for always being there.

Last, but certainly not the least, I thank my parents for their unwavering support and for believing in me. I thank my father for being my strongest ally and my mother for being my biggest advocate, as they have gone above and beyond to help me pursue my goals. Words will never be enough to express the depth of my gratitude for everything they have done for me.

TABLE OF CONTENTS

Page

APPENDICIES

LIST OF ILLUSTRATIONS

Figure Page

LIST OF TABLES

Table Page

1. INTRODUCTION

Privacy protection often involves human decision making from the user and the agency they are interacting with. Often these decisions about what should be protected, what needs to be protected, and when protection should be enforced, are based on a complex set of factors and bodies of knowledge. For example, there are significant individual differences in regards to how people value their privacy and share their information (Berscheid, 1977) and these values may change across different contexts (Tsai, Egelman, Cranor, & Acquisti, 2011; Spiekermann, Grossklags, & Berendt, 2001). Studies also found that people value privacy but behave in a way that jeopardizes that value (Tsai et al., 2011; Spiekermann et al., 2001). The focus of this study was to gain a deeper understanding of how users respond to smart appliance privacy related information and potential threats to privacy by examining their attitudes towards privacy and their behavioral intent to protect their information. Privacy policies utilizing varying degrees of abstractness were created and used in this study. The policies showcased different components to provide privacy information and were compared to the traditional policy format. The research sheds light on the possibility that privacy attitudes and related behaviors are not clear cut and are potentially impacted by the technology literacy of users by utilizing a moderated-mediation analysis. It adds to existing literature by bringing attention to the idea that current privacy policies may not sufficiently enable users to make privacy conscious decisions.

Social networking, online purchasing, web browsing, and internet connected devices have become a ubiquitous part of life. The Center for the Digital Future (2015) reported that Americans spend approximately 21.5 hours online per week. This value has increased to 23.6 hours online per week (The Center for the Digital Future, 2017). Online behavior (such as social media, browsing the internet, shopping on various websites, etc.) is shaped by perceptions of privacy and security (Ponte, Carvajal-Trujillo & Escobar-Rodríguez, 2015). People are concerned about both privacy and security when they are online (Hoffman, Novak, & Peralta, 1999; Metzger & Docter, 2003). For the purpose of this research, security is defined as the measures undertaken to protect connected devices and the information they collect from unauthorized access over the internet. This is generally achieved via proprietary encryption software that the consumer has little or no control over. Privacy is defined in many ways, but for the purpose of this research, it is conceptualized as an individual's ownership, control over sharing, and protection of their personal information. This personal information is subject to sharing across various platforms and devices. Due to the broad scope and depth of concerns in both the areas of security and privacy, it was necessary to choose one area as the focus of this study. Privacy was selected as it is a concept that focuses around the individual user's perception, understanding, and decision-making abilities, and because individuals have more control over it.

Over the years, privacy concerns have continued to grow instead of reduce (Ackerman, Cranor, & Reagle, 1999). Privacy disclosure statements currently in use represent current methods used to inform users about how companies protect and share consumer information. The presence of privacy statements on websites make people more willing to provide their personal information (Hoffman et al., 1999). Individuals evaluate the risk of sharing their information and estimate the degree to which their privacy is protected, by taking into account the presence of privacy statements and the level of control they have over sharing their information, which in turn determines how much information they share on online sites (Ray, Ow, & Kim, 2011; Metzger, 2004). At the same time, Metzger (2004) argues that individuals who spend more time online share more information and are less concerned about privacy than individuals who spend less time online.

A great deal of privacy and information disclosure research has focused on behavior with web-based applications and social media contexts, while less research has examined privacy and information disclosure related to the emerging market of appliances that connect to applications on users' smartphones via an internet connection such as the GE WiFi Connect appliance range, Samsung's CHEF collection, and LG's SmartThinQ. These appliances require users to make decisions about how they share their personal information that they have entered with other appliances within their home, with vendors, and with third party companies outside their home. Currently, the extent to which users can comprehend privacy disclosures statements is not understood within this particular context.

Current research is focused on designing smart homes that have the ability to monitor the resident's daily activity (Ding, Cooper, Pasquina, & Fici-Pasquina, 2011). Research is also focused on the integration of smart appliances and sensors to ensure that smart homes afford a safe living environment (Tsai, Chien, & Cheng, 2003). Smart homes are being developed with the capability to function autonomously without the need for full user control and command (Montano, Lundmark, & Mahr, 2006). Montano et al. (2006) suggested that smart homes can improve security but the complex systems required can affect privacy. Product developers have the knowledge and skills to understand the complexity of these systems. However, a user who purchases this technology needs to use supplemental information to understand the system. This supplemental information is provided through technical manuals that accompany the appliance. Internet connected devices, such as smartphones, have start up screens that guide the user through the setup process. As the user progresses through the screens, he or she is prompted to agree to the terms and conditions prior to using the device so that he or she can access the device. It is likely that smart appliances will have similar setup procedures.

Online privacy statements ask users to check a box to indicate that the privacy statement has been read. Sometimes the privacy statement is right there and sometimes it is a separate link. However, there are no checks and balances to ensure the privacy statement has been read, merely that it has been opened. McDonald and Cranor (2009) estimated that it could take an individual approximately 201 hours per year to read privacy policies. This is a lot of time that consumers would spend reading privacy policies that provide information regarding how personal information is collected, stored, shared, and used. In addition to time barriers, privacy policies are also difficult to understand (Jensen & Potts, 2004; Tsai, et al., 2011). For example, Turow, Feldman & Meltzer (2005, p. 4) found that 70% of the respondents did not agree that “privacy policies are easy to understand” when they questioned adults who used the internet, regarding website privacy policies.

The problems associated with time barriers and reading comprehension are exacerbated with the mere presence of privacy disclosure statements. Research by Turow et al. (2005) showed that surveyed individuals believed the presence of a privacy policy meant their personal data was protected. However, any document labelled a privacy policy does not automatically mean that appropriate steps are taken to protect and maintain an individual's privacy. Turow et al. (2005) argue that in actuality individuals might not have enough information to make informed decisions when it comes to protecting their privacy and disclosing their information even if the website or company has a privacy policy. Additionally, research by Tsai et al. (2011) showed that individuals needed salient privacy information indicators such as icons indicating high or low privacy to know if the website offered low or high levels of privacy protection. In their experiment, the researchers utilized the Privacy Finder tool, which is a search engine that annotates online search results with a privacy meter icon. This tool was used to analyze computer-readable online privacy policies and generate icons. These icons indicated whether websites offered low, medium, or high privacy, which enabled people to make decisions regarding visiting and using that website. Users' tendencies to make decisions about privacy and personal information disclosure based on incomplete information may be best understood by examining extant literature on the concept of bounded rationality.

1.1. BOUNDED RATIONALITY AND PRIVACY DECISIONS

The concept of bounded rationality is attributed to Herbert A. Simon (1957). In lay terms, bounded rationality explains that an individual's decision making abilities are affected by cognitive limitations in acquiring and processing the information available, and time constraints faced to process all the information, before coming to a decision (Simon, 1957). A fully rational individual is able to make correct decisions regardless of the complexity of the situation and they arrive at sound conclusions every single time in the decision making process (Selten, 1999). Bounded rationality in simple terms is the absence of full rationality, but it is not complete irrationality. As the individual is exposed to information, he or she adapts to real-world situations and the theory of bounded rationality is used to explain adaptation under cognitive bounds (Gigerenzer & Goldstein, 1996). Individuals are aware of minimum information and do not go above and beyond to learn more information, as they do not feel the need to gain the maximum outcome obtained by making a fully informed decision. It makes intuitive sense that individuals want to avoid making poor choices. When faced with complex problems, more thought is required in order to solve the problem successfully. However, there may still be insufficient insight to solve the problem within that context, which in turn impacts the decision made (Parker & Tavassoli, 1997). Bounded rationality is likely to play a role in explaining the divide that exists between consumers' privacy attitudes and actual behavior. Some recent findings related to this are highlighted below.

Consumers may not take the time to review the information provided as shown by results of the experiment conducted by Acquisti and Grossklags (2005). In their experiment, participants were asked to fill out an online survey that questioned attitudes towards risks, knowledge of risks, past behaviors related to protecting and releasing personal information, and attitudes towards privacy. Nearly 90% of the respondents were moderately concerned or very concerned about privacy. Respondents were more concerned about giving out identifying information such as names and emails than profiling information such as profession and weight. Respondents showed incorrect or lack of knowledge regarding privacy risks, methods for protecting their privacy, and existing privacy legislature. Forty-one percent of the individuals highly concerned about privacy admitted to rarely reading privacy policies.

It is possible that consumers do not read privacy policies because they are unable to understand the language used or the manner in which the information is presented is complicated. Arguably, most individuals do not read such documents on a daily basis and, perhaps, when the time comes to review privacy policies, the individual is more concerned with using the online platform or device. In other words, consumers may have access to the necessary information but they either ignore it or do not understand it, and therefore, do not make correct choices concerning their privacy. There are many factors that affect the decision making process such as knowledge, attitudes, trust in vendors, and finances. The consumer's knowledge is built upon the information he or she has access to. If the information is incomplete it can affect the privacy decision. Privacy policies, terms and conditions, and privacy disclosures are just some of the numerous ways companies disclose information to consumers regarding how consumer information is collected, stored, secured, and shared. Despite the availability of and access to all this information, consumers are limited with respect to bounded rationality, which affects their understanding of all the details provided to them because of bounded rationality (Acquisti & Grossklags, 2005).

Furthermore, Acquisti and Grossklags' (2005) experiment showed that respondents' attitudes about privacy contradicted the manner in which they shared information. The level of importance given to privacy was correlated to concern for privacy, but these responses were not reflected entirely when it came to actual behaviors. Results of their study showed that 67% of the respondents did not encrypt their emails, 21.8% revealed their social security numbers for discounts and services, and 28.6% gave their phone numbers during interactions with vendors and a variety of other contexts provided in the experiment. Studying privacy concerns and signing up for loyalty cards, revealed that 87.5% of the respondents who had high concerns regarding sharing their information signed up for such services by providing their personal identifying information. It is possible that the respondents engaged in a risk-rewards trade-off and shared their personal information as the rewards appeared beneficial (signing up for loyalty cards) and the loss of privacy did not seem risky.

It raises the question about whether people really understand what happens when they share their personal information. Acquisti and Grossklags (2005) argue information is stored and shared in ways that most consumers are unaware of since the researchers found that almost half of them do not read privacy statements. Even with access to privacy disclosure information, consumers made decisions that counter their attitudes regarding privacy. Arguably, the individual's ability to process all the available information regarding privacy at once is limited as certain privacy cues are being followed while others are being ignored. Bounded rationality provides an explanation as to why people deviate from making rational choices even with access to complete information because people have no context or frame of reference to process and understand the information, and are not motivated to obtain it if the risks are not apparent. This hampers their ability to make correct decisions and further impedes their ability to understand the consequences of their decisions.

In another example of how consumers make non-rational decisions, the experiment by Spiekermann et al. (2001) compared self-reported privacy preferences to the individual's actual information disclosing behavior. In their experiment, participants shopped for one of two products and were provided with an incentive such as a 60%

discount on all products available at an online store. The online store was created for the experiment and the participants were informed that the study was being done to develop a search engine. The participants were able to communicate with an anthropomorphic program bot by asking it questions to obtain information. Otherwise, they could simply look at product descriptions to get the information they needed. Participants were provided with either one of two privacy statements. In condition one, the privacy statement informed participants that a reputable company would receive all their navigational data. In condition two, the privacy statement informed the participants that their data would be given to an entity unknown to the researchers. The participants in condition two were also informed that the researchers did not know how the participant’s data would be used. The researchers measured self-disclosure based on the quantity of information exchanged and disclosed by the participants. They found that participants readily revealed private and personal information while communicating with the anthropomorphic bot, even when they were part of condition two that informed them their information would be sent to an unknown entity. Participants did not significantly alter their communication with the bot as it asked them questions. Based on their self-reports, the researchers categorized some participants as particularly reserved about sharing their information. However, these participants did not act in accordance with being reserved. The amount of information these particular participants had disclosed could be used to construct a revealing consumer profile. The participants were willing to talk about themselves with the bot and they did not engage in privacy-conscious behaviors, indicating that the study participants do not behave in the way they say they would. Spiekermann et al. (2001) suggests that participants may have had more trust in the data protection offered even though there was no clear description of the type of data protection provided, if any at all. However, this explanation is inadequate as it does not entirely explain the divide between participant's attitudes regarding privacy and their actual behavior.

It makes little sense that an individual would share personal information with an anthropomorphic bot. However, bounded rationality can provide an explanation as to why the individual does not understand how the collected information is going to be shared or chooses to ignore privacy statements that explain sharing protocols. The individual has no point of reference to explain what the unknown entity could do to their information. The privacy statement in condition two mentioned that the researchers were unware of how the data would be used (Spiekermann et al., 2001). An argument could be made that the participants did not have an idea of how the data could be used or misused. Therefore, their decision making ability was reduced due to the limited information provided and the participants' own knowledge.

Chellappa and Sin (2005) examined the dilemma consumers' deal with when trying to personalize their information online and maintain their privacy, which serves as another example of how consumer decisions reduce in rationality. The more trust consumers have in the source of information could mean they have less rational thoughts about the information itself. In the sense that, the consumers do not think reasonably about the information and results of their actions, because they place a high value and trust on the services. The researchers argued that while consumers have concern for their privacy, they are willing to share their information in exchange for benefits such as receiving personalized services and convenience. The researchers measured the value consumers placed on personalization regarding product browsing, purchasing experience, and services. They also measured privacy concerns regarding collection of identifiable and unidentifiable information. Participants answered surveys that were presented to them as being from online firms belonging to the automobile, apparel, financial services, personal computers, or travel services industries. They found that the value consumers placed on personalization impacted their decision to use the personalization services. When the consequences of the services became more meaningful to the consumer, their rationality regarding the situation reduced, as the consumer focused on gaining benefits. The consumers were not provided with the information about the immediate outcomes of their actions such as loss of privacy, and were probably unable to make those connections due to bounded rationality of their thought process. It was difficult to determine if the amount of use of personalization services was due to the value placed on it or the idea of sharing personal information. Both those factors play a role and if the vendor is able to gain the trust of the consumer, then there is an increased chance the consumer will use the personalization services. If trust is present and the consumers see more value in using the services, then they will share their personal information even if they are concerned about privacy. This raises the question of whether the consumer has understood the downside of the tradeoff they saw as beneficial. People share their information willingly if they think that the benefits outweigh the loss of privacy and if they trust the vendor.

Consumers engage in a cost-benefit analysis, but it is difficult to determine if they are able to carry out this analysis effectively and correctly (Chellappa & Sin, 2005). Information the consumer has access to is limited, and they might not be able to imagine the ways in which their personal information can be used and shared with other parties.

Bounded rationality plays a role in explaining the less rational decision making of consumers in deciding the actual cost incurred due to the loss of their personal information. There are no written examples and contexts consumers can refer to in order to gain knowledge on the drawbacks of sharing information just to gain some benefit of using personalized services.

In order to develop a measure for privacy attitudes related to smart appliances, validated measures were reviewed. The Concern for Information Privacy (CFIP) scale, published by Stewart and Segars (2002), measured four dimensions of collection, improper access, errors, and unauthorized secondary use, related to online privacy. From this scale, it was seen that concern for privacy is multidimensional and this was taken into account while developing the survey items for this variable. Xu and Teo (2004) proposed a model to measure privacy concerns regarding location based services. From their model, the items used in the privacy concern measure regarding how information could be used by other companies was a concept that was incorporated into the current survey items as well. Both these measures formed the bases for the items used in the privacy attitudes questionnaire, used in this experiment. Additionally, it was essential to take into account the technology literacy of individuals. Technology familiarity can create a divide among users which leads to a gap between privacy behaviors (Park, 2013). As such, some users are more familiar with and accustomed to using technology, while others are not and engage in different privacy related behaviors.

It is important to examine methods to help consumers make decisions that better reflect their attitudes. A method proposed in this research is the use of examples which have varying degrees of abstractness that explain sections of privacy policies such as networking appliances, voice recognition, and social media in lay terms. Components of a privacy policy that varied in abstractness were created (referred together as Abstractness of Privacy Disclosures). Two of these components consisted of examples that were grounded with relevant and plausible applications to real world situations. These examples can help create better contexts that more accurately reflect actual privacy risks with respect to user behavior and, in turn, smart appliance usage. These components can help users make appropriate decisions after they have understood the greater scope of privacy policies using the examples. With the impending ubiquity of smart home technologies and smart appliances, the level of information sharing these technologies will demand make it unlikely that consumers will be able to manage privacy protection in a manner that reflects their actual attitudes. This could lead to emotional, social, and economic hardship for ill-informed users. Therefore, it is a critical time to develop an approach to privacy statements and disclosures that reflect limitations related to bounded rationality so that users do not carry the entire burden of managing policies that are often meant to protect and benefit the retailer.

1.2. HYPOTHESES

With smart appliances being introduced into the market, it is important to know if there is a purchasing interest for such appliances. By providing information about smart appliances and their features along with possible risks, all relevant pieces of information are present in order for consumers to make a decision regarding purchasing smart appliances. Consumers are interested in the benefits and when they find the benefits meaningful, they share their information (Chellappa & Sin, 2005). It is important to find out whether, when given access to information regarding potential risks that may occur after sharing personal information, if the interest in purchasing smart appliances changes. Participants selected the aspects of smart appliances that appealed to them and their likelihood of purchasing smart appliances (Appendix D). The Abstractness of Privacy Disclosures (Traditional Content, Traditional Content + Neutral Examples, Neutral Examples, Neutral Examples + Risk Examples, Control) provide some of the benefits and risks in lay terms and legal verbiage depending on which of the five conditions is read. As such, it was hypothesized:

Hypothesis 1: The Likelihood of Purchasing Smart Appliances differs across Abstractness of Privacy Disclosures.

Attitudes form based on available information and experience (Fazio, Zanna, & Cooper, 1978). Individuals who are familiar with the everyday technology they use and are able to use the technology effectively without being frustrated are referred to as individuals who are skillful with technology. Such individuals may have a better understanding of how the programs and devices work, and use their knowledge to form their attitudes about the technology they use. They may have a better grasp of the definition of certain terms they come across when they are setting up their accounts and using their devices. Whereas, individuals who cannot use devices and programs effectively and efficiently may not be as proficient. Such individuals may be at a disadvantage in terms of understanding technical terms they come across while they use their devices, even if the information is provided in lay terms. Technology literacy and available experience may impact the attitudes developed about privacy. As such, it was hypothesized:

Hypothesis 2: Technology Literacy will moderate the relationship between Abstractness of Privacy Disclosures and Privacy Attitudes, such that as the privacy disclosure becomes less abstract, Privacy Attitudes will increase particularly for those high in Technology Literacy.

By providing people with less abstract information regarding smart appliances' privacy policies, individuals may have a better grasp of what they stand to gain and lose and their privacy attitudes may change. As the privacy attitudes change, it is possible that less personal information is shared. Privacy attitudes may explain why less information is being shared depending on the type of Abstractness of Privacy Disclosures. As such, it was hypothesized:

Hypothesis 3: Privacy Attitudes will mediate the relationship between Abstractness of Privacy Disclosures and Privacy Behaviors, such that less abstract privacy disclosures will drive an increase in Privacy Attitudes, which will in turn predict a decrease in sharing Privacy Behaviors.

2. METHODS

2.1. PARTICIPANTS

The study was conducted using an online survey built in Qualtrics and launched on Amazon Mechanical Turk (MTurk). Participants were recruited via MTurk. This provided a demographically diverse sample population that varied in age, gender, and academic backgrounds rather than collecting data utilizing available college students. If the study included college students from Missouri University of Science and Technology, it could have limited the diversity of the sample since a majority of students study engineering. Engineering students may have more knowledge about smart appliances, technology, and related fields due to their academic discipline compared to the average population, which could impact the results. Therefore, MTurk was utilized and care was taken to ensure that the MTurk workers participated only once in the study to prevent repeat responses.

A total of 188 participants completed the survey. Participants were compensated for their time and effort with $1.75. This amount was approved by the campus Internal Review Board (IRB). On average, the participants took approximately 15 minutes (*SD* = 8.14 minutes) to complete the survey. As this research involved human participants, it was necessary to maintain the safety and confidentiality of their participation. The study proposal received IRB approval and all subjects remained anonymous as they participated in the survey. Slightly over half of the participants were male (51.6%) and the average age of the population was 40.63 years (*SD* = 11.31 years). Participants were from a variety of educational backgrounds such as business, healthcare, sciences (physics, chemistry, biology, computer science, etc.), arts, languages, education, design, engineering, and religious studies, to name a few. The average work experience was 17.33 years (*SD* = 11.1 years) and the participants worked in diverse fields of healthcare, law, business and finance, real estate, administration, forestry, human resources, and others.

2.2. MEASURES

For this study, a vignette about a fictional company “Smartenna” was created. Participants were led to believe that Smartenna provides a range of internet-connected technologies that could improve quality of life and provide ease of access for many services such as social networking and customized content. Participants were then presented with a fictitious privacy agreement, and privacy attitudes, privacy behaviors and technology literacy items, as described below.

2.2.1. Abstractness of Privacy Disclosures. Privacy disclosures are the current means through which individuals are notified about how their information is collected, stored, and used. To explore how varying abstractness (increase in concreteness) impacts privacy attitudes and behaviors, three different components of a privacy disclosure were devised for the fictional company – Traditional Content, Neutral Examples, and Risk Examples. The Traditional Content was a typical privacy policy and disclosure statement (Appendix A) created using concepts and verbiage from the privacy policies of popular social networking sites such as Twitter, appliance manufacturers such as Samsung, VIZIO, and GE, and device manufacturers such as Fitbit. The Neutral Examples consisted of three examples, specifically about connected devices, voice recognition, and social media (Appendix B), illustrating how Smartenna appliances could use consumer data but did not explicitly highlight the risk, for example:

Aaron has several smart appliances connected to his smartphone Smartenna application. He uses customized settings on his connected appliances to save energy and money. Aaron hires Susan to house sit for a short period of time during summer vacation. He authorizes Susan's smartphone so she can control the smart appliances while he is away. Susan can see how Aaron operates his appliances so that she can operate them the same way while he is gone to continue his energy savings plan – including washer/dryer cycles settings, dishwasher settings and usage times, ordering product refills, etc.

The Risk Examples consisted of three examples of how the information shared through Smartenna appliances could be misused (Appendix C). These examples were also related to connected devices, voice recognition, and social media, and built upon the Neutral Examples, for example:

About 10 months later, Susan messages Aaron that she is available to house-sit over the summer again and sends him a gift basket containing his favorite coffee brand, specialty coffee creamers, and nutrition bars. Aaron is certain he didn't mention these favorite items to Susan, and when he asks about it she mentions that while she house-sat, she noticed he had purchased these products in the past via the Smartenna application history for his fridge and coffee maker.

2.2.2. Distraction Task. A distraction task was created to learn about participants' attitudes about smart appliances regarding the prospect of purchasing smart appliances (Likelihood of Purchasing Smart Appliances), selecting smart appliances they would like to use and features they have a preference towards (Appendix D). The participants provided their responses based on a 5-point Likert scale for respective items.

2.2.3. Privacy Attitudes. For the purpose of this research, privacy attitudes was defined as the concern given to privacy on an individual basis regarding companies, users, and personal information. This part of the survey contained 16 items regarding how concerned individuals are about the use of the data they provide to companies and how concerned individuals are about providing information to service providers (Appendix E). The questionnaire was created for the purpose of this study. As described in the Introduction, the measures were based on items from the CFIP scale (Stewart & Segars, 2002) and concern about location based services (Xu & Teo, 2004), and were modified as needed to fit the smart appliances framework used in this study. The participants provided their responses based on a 5-point Likert scale for respective items.

2.2.4. Privacy Behaviors. For the purpose of this research, privacy behaviors was defined as the choices individuals make to maintain their privacy and share their personal information. The privacy behaviors questionnaire (Appendix F) was created for the purposes of this study. The items were developed based on the type of the information that was readily shared as discussed in the Introduction (Acquisti & Grossklags, 2005). It aimed to capture the degree to which individuals would be willing to share personal information (such as name, date of birth, email, home address, phone number, etc.) across three different contexts including online shopping, signing up for membership and rewards programs, and filling out warranty and product support information. These three contexts were selected because it is likely that these are behaviors individuals will engage in when purchasing and using smart appliances. Additionally, past behaviors regarding social media privacy settings were captured and participants were asked if they were likely to change these settings. The latter question could provide the grounds for evaluating whether individual behaviors might change when given different combinations of the three components from the Abstractness of Privacy Disclosures. The participants provided their responses based on a 5-point Likert scale for respective items.

2.2.5. Technology Literacy. For the purpose of this research, technology literacy was defined as the degree to which an individual can easily and effectively use technology. By using technology well, individuals can gather knowledge about the features the technology offers. Therefore, it was necessary to capture the technology literacy of the participants. For this purpose, a short set of questions was created and was based on technology and related tasks individuals partake in on an everyday basis, as listed in Appendix G. The participants provided their responses based on a 5-point Likert scale for respective items. These questions aimed to capture the ease individuals felt when using different devices and programs. All these questions were related to simple everyday tasks of using computers, emails, and programs such as word processor and spreadsheet software. Additionally, it captured the individuals' perceptions of their own technology proficiency in relation to others. As such, the participants' technology literacy was calculated in regards to hardware, social media, software, comparative knowledge, and frustration.

2.3. DESIGN

This study utilized a between-subjects design with Abstractness of Privacy Disclosures as the independent variable, Technology Literacy as the moderating variable, Privacy Attitudes as the mediating variable, and Privacy Behaviors as the dependent variable. Participants responded to items that captured their privacy attitudes and behaviors. These items varied in the order they were presented to reduce order effects. By counterbalancing the design, groups of participants in each condition received the items of each variable in different orders.

For the Abstractness of Privacy Disclosures, the impact the three components on aligning privacy behaviors to privacy attitudes (henceforth referred to as consistency) were measured individually and in combination with one another in four conditions: Traditional Content, Traditional Content + Neutral Examples, Neutral Examples, Neutral Examples + Risk Examples. It was expected that the Traditional Content condition would produce findings that mirror existing research highlighted in the literature review with respect to consistency. The Traditional Content + Neutral Examples represents a reduction in the abstractness of information provided in the policy because it provided a context for the legal verbiage and therefore could potentially increase consistency. However, it was possible that adding Neutral Examples to the Traditional Content could have resulted in a negative impact on consistency because it added even more information to a task that users are already not doing well in. Therefore, the third group received the Neutral Examples by itself. In this condition, participants had the option to expand the corresponding Traditional Content section, if they so desired. This provided the participants with the opportunity to read the actual policy if they wanted to but did not flood them with extra text upfront. It was also possible that the Neutral Examples would still be too abstract, so a fourth condition was tested in which Neutral Examples and Risk Examples information were presented together. The participants in this condition also had the opportunity to expand the corresponding Traditional Content section. The Risk Examples condition by itself would appear out of context, and therefore it was not tested on its own. Additionally, the Traditional Content + Risk Examples condition was not presented as a condition because it was highly unlikely that a company would just add a description of risks, i.e. provide consumers with a privacy policy and what could go wrong, since companies want to attract consumers. A control condition was used as well. The participants in this group did not receive any of the manipulations in order to create a condition where participants were forced to ignore the privacy policy. Instead the control group received the following piece of information about Smartenna:

Smartenna has created a collection of internet-connected appliances and technologies that make the home convenient. This collection includes refrigerators, dishwashers, washing machines, dryers, thermostats, etc. Smartenna appliances offer features such as connections to social networks, customized content, service and product recommendations, and supported applications. These features can be customized based on the owner's interactions with the appliance. Smartenna appliances improve user experience and provide ease of access for many goods and services. To improve functionality of these appliances owner data is collected, used, stored, shared, and protected through each appliance.

2.4. PROCEDURE

Participants first read the Smartenna vignette (see Introducing the Smartenna Product Line in Appendix A). Then, participants were invited to read one of the five conditions that they were randomly assigned. The group that received the Traditional

Content was used as the reference condition for all the analyses that were conducted because this condition represented the current methods used to provide information to consumers, while the other conditions (Control, Traditional Content + Neutral Examples, Neutral Examples, and Neutral Examples + Risk Examples) manipulated the abstractness (increased concreteness of information). Additionally, after reading their respective conditions, the participants were provided with the following definition of smart appliances (see complete definition in Appendix D):

Smart appliances are appliances that connect to your smartphone or computer, and provide you with controls to manage appliances from wherever you are. These connections are made using Wi-Fi and have a variety of settings that can be customized to the owner's needs.

This definition was developed based on the appliances currently available on the market that are labelled as smart appliances such as the GE WiFi Connect appliance range, Samsung's CHEF collection, and LG's SmartThinQ. By defining smart appliances, all participants were provided with the same understanding of what this term means and it controlled for any variance that might have occurred if participants answered the survey without a full idea of what smart appliances mean within the context of this study. Following this, the participants were provided with the Distraction Task, to reduce the impact of participant bias and to prevent them from figuring out the true purpose of the experiment. Then, they responded to items in the Privacy Attitudes questionnaire and Privacy Behaviors questionnaire, respectively. Lastly, they responded to items in the Technology Literacy questionnaire and answered demographic questions.

3. RESULTS

3.1 SCALE DEVELOPMENT

The items from each questionnaire were analyzed or grouped into dimensions.

3.1.1. Privacy Attitudes. A factor analysis using principal axis factoring extraction and direct oblimin rotation indicated that 16-item questionnaire loaded onto 4 different factors (see Table 3.1.). Item 10 loaded -.25 for Factor 1 and < .15 on Factors 2, 3, and 4, and was removed from the factor analysis. The 15 items that loaded for each factor were converted into factor scores using SPSS (version 25). The Concern about Information Misuse factor score consisted of 4 items (α = .94) and the Companies and Users Do Not Devote Time and Resources for User Protection factor score consisted of 4 items (α = .80). The Companies Should Not Use, Share, and Sell User Information factor score also consisted 4 items (α = .77) and the Concern about Personal Information factor score consisted of 3 items (α = .86). To facilitate an understanding of these factors, a high score on any of these items corresponded to a high concern for privacy. For example, a high score on Concern about Information Misuse items indicated that participants were highly concerned about their privacy in regards to the possibility of their information being used for purposes they were not approved for. To reduce the number of variables included in the final analysis, Companies and Users Do Not Devote Time and Resources for User Protection was excluded, while the other three factor scores were retained. These three factor scores were selected since they were about the concern for information being misused or sold, while the excluded factor was concerned with resources and time spent on protecting information.

Table 3.1. Factor Loadings Based on Principal Axis Factoring with Direct Oblimin Rotation for 15 Items from the Privacy Attitudes Questionnaire.

	Item Loadings			
Items	1	2	3	4
Concern about Information Misuse				
13. I am concerned that the information I submit to the smart appliance could be misused.	**.913**	.028	-.022	.009
15. I am concerned about submitting information on the smart appliance because of what others might do with it.	**.889**	.085	-.007	.014
16. I am concerned about submitting information on a smart appliance because it could be used in a way I did not foresee.	**.865**	.021	-.012	.084
14. I am concerned that a person can find private information about me because of a smart appliance.	**.779**	-.048	.106	.024
Companies and Users Do Not Devote Time and Resources for User Protection				
5. Users devote appropriate resources towards preventing illegal access to personal information on smart appliances (such as reading policies, changing passwords, customizing privacy settings).*	-.037	**.851**	.033	-.120
8. Users take steps to make sure that hackers cannot access the personal information in their smart-appliances.*	.003	**.712**	.026	-.083
4. Companies and manufacturers of smart appliances devote appropriate resources (such as time, money, effort) to protecting my personal information.*	.116	**.680**	-.093	.061
7. Companies and manufacturers take steps to make sure that hackers cannot access the personal information in their smart appliances.*	.003	**.582**	.029	.162
Companies Should Not Use, Share, and Sell User Information				
12. Companies should never share personal information with other websites or companies unless it has been authorized by the individuals who provided the information.	-.030	.029	**.850**	-.010
9. Smart appliance companies should not use personal information for purposes that have not been authorized by the individual who provides the information.	.140	-.062	**.649**	-.130

Table 3.1. Factor Loadings Based on Principal Axis Factoring with Direct Oblimin Rotation for 15 Items from the Privacy Attitudes Questionnaire (cont.).

	Item Loadings			
Items	1	2	3	4
11. Company databases should never sell the personal information they have collected to third party vendors.	-.051	.044	**.617**	.182
6. Databases that contain personal information collected from smart appliances should be protected from illegal access – no matter how much it costs.	-.012	.024	**.571**	.096
Concern about Personal Information				
1. Generally speaking, it bothers me when websites ask me for personal information.	.101	.028	-.030	**.831**
2. Generally speaking, when websites ask me for personal information, I think twice before providing it.	-.006	-.022	.137	**.701**
3. Generally speaking, I am concerned that websites are collecting personal information about me.	.250	-.013	.040	**.669**

Note. * Indicates item was reverse scored.

Table 3.2. Privacy Behaviors Information Sharing Frequency Score.

Information	Shared	Frequency	Sharing Behavior	Implication
Name	Yes = 1	Always = 5	1 × 5 = 5	Always shares name
Name	Yes = 1	Most of the time = 4	1 × 4 = 4	Mostly shares name
Name	Yes = 1	Sometimes = 3	1 × 3 = 3	Sometimes shares name
Name	Yes = 1	Rarely = 2	1 × 2 = 2	Rarely shares name
Name	Yes = 1	Never = 1	1 × 1 = 1	Shares name infrequently
Name	No = 0	0	1 × 0 = 0	Never shares name

Note. Repeated across each of the three contexts to compute a total of 24 sharing behavior frequency scores.

3.1.2. Privacy Behaviors. The frequency of sharing personal information was calculated in order to get a full understanding of the extent sharing behaviors in regards to which particular pieces of information get shared the most. Table 3.2. provides an example of how the calculation was conducted. It is important to note the distinction between "no" and "never." If an individual selected "no," it was understood that this person did not share their name at all in that context. However, if an individual selected "yes" and "never", then it was understood that this person did share their name infrequently for online shopping or other contexts, even less than a rare occasion. Due to the large volume of information gathered in the privacy behaviors questionnaire, the items related to social media sharing behaviors were not analyzed. After computing the sharing behavior frequencies across all three contexts, there were a total of 24 items. Social security number was not shared under any of the three contexts and was removed from the analysis.

A factor analysis using principal axis factoring extraction, direct oblimin rotation and four fixed loadings was used for the remaining 21 items (see Table 3.3.). The items that loaded for each factor were converted into factor scores using SPSS (version 25). The Contact Information factor score consisted of 12 items (α = .91), the Purchasing History factor score consisted of 3 items (α = .89), the Date of Birth factor score also consisted of 3 items (α = .90), and the Financial Information factor score consisted of 3 items (α = .87). A high score on any of these factors indicated that participants had a higher frequency of sharing that piece of information. To reduce the number of variables in the final analysis, only the Contact Information factor score was used because it contained the items (name, email, home address, and phone number) that are widely used and often required in the three context – online shopping, membership and rewards programs, and warranty and product support.

3.1.3. Technology Literacy. Technology literacy was organized into Hardware Technology Literacy (5 items – 1a to 1e, α = .83), Social Media Technology Literacy (4 items – 2a to 2d, α = .80), Software Technology Literacy (6 items – 3a to 3f, α = .80), Comparative Knowledge Technology Literacy (4 items – 5a to 5d, α = .88), and Frustration Technology Literacy (5 items – 6a to 6e – reverse coded, α =.89). For each participant, mean scores were calculated for the five types of technology literacy. By calculating the mean scores, the technology literacy scores were computed only for the items that participants rated themselves on. For example, if participants responded they found Facebook and Twitter easy to use, the mean of the scores for these two item was calculated. Participants were not docked points for not using a device, program, or social media platform. Their technology literacy was computed based on what devices, programs, and social media platform they used. Mean scores were calculated for each participant to provide a value of their technology literacy for each of the five dimensions.

A high mean score on any of these dimensions corresponded to a high technology literacy for that dimension. For example, a high Hardware Technology Literacy score indicated that the participant was easily able to use smartphones, computers, laptops, tablets, and gaming systems. After reverse coding the items for frustration technology literacy, a high score indicated that the participants were not frustrated when using social media, smartphones, and computer programs. To reduce the number of variables in the analysis, Frustration Technology Literacy was excluded as it contained items that cut across hardware, social media, and software technology literacy.

Table 3.3. Factor Loadings Based on Principal Axis Factoring with Direct Oblimin Rotation for 21 Items from the Privacy Behaviors Questionnaire.

	Item Loadings			
Items	1	2	3	4
Contact Information				
Sharing email online frequency score	**.800**	-.016	.167	.024
Sharing phone number online frequency score	**.705**	-.050	.039	.141
Sharing home address online frequency score	**.679**	-.276	.079	.176
Sharing name online frequency score	**.678**	-.116	-.110	.015
Sharing email for MR frequency score	**.657**	.130	-.035	-.103
Sharing home address for WPS frequency score	**.640**	.171	-.106	-.065
Sharing home address for MR frequency score	**.637**	-.047	-.143	.133
Sharing phone number for MR frequency score	**.634**	.109	-.041	.074
Sharing email for WPS frequency score	**.626**	.214	-.059	-.192
Sharing name for WPS frequency score	**.617**	.145	-.220	-.200
Sharing name for MR frequency score	**.566**	.119	-.283	-.136
Sharing phone number for WPS frequency score	**.515**	.224	-.071	-.012
Purchase History				
Sharing PPI for MR frequency score	.095	**.853**	.070	.153
Sharing PPI for WPS frequency score	-.014	**.740**	-.044	.095
Sharing PPI for online frequency score	.087	**.730**	.031	.216
Date of Birth				
Sharing DoB for MR frequency score	.053	-.052	**-.927**	.006
Sharing DoB for WPS frequency score	-.041	.008	**-.865**	.030
Sharing DoB for online frequency score	.072	-.090	**-.730**	.192
Financial Information				
Sharing income for MR frequency score	.033	.144	-.087	**.811**

Table 3.3. Factor Loadings Based on Principal Axis Factoring with Direct Oblimin Rotation for 21 Items from the Privacy Behaviors Questionnaire (cont.).

	Item Loadings			
Items	1	2	3	4
Sharing income for online frequency score	.060	.175	-.130	**.693**
Sharing income for WPS frequency score.	-.001	.259	-.141	**.591**

Note. MR = Membership and Rewards Programs; WPS = Warranty and Product Support; DoB = Date of Birth.

3.2. DESCRIPTIVES

Descriptive statistics and correlations for the variables across the five conditions are included in Table 3.4. In terms of privacy attitudes, concern regarding Companies Should Not Use, Share, and Sell User Information" (ComUInfo) significantly increased in the Control condition ($r(186) = .152$, $p < .05$) when compared to the other four conditions. This indicated that in the Control condition, participants concern about how companies used, shared and sold their information was higher compared to the other conditions. Concern about Information Misuse (CInfoMis) significantly decreased in the Neutral condition ($r(186) = -.200$, $p < .01$) when compared to the other conditions. This indicated that in the Neutral condition, the participants' concern about the information being misused decreased when compared to other conditions.

3.3. HYPOTHESES

First, to test H1 that Likelihood of Purchasing Smart Appliances differed across Abstractness of Privacy Disclosures, a one-way ANOVA of condition on Likelihood of Purchasing Smart Appliances was conducted. There was a statistically significant effect of conditions $F(4,179) = 2.696$, $p = .032$, $\eta_p^2 = .057$, in partial support of *H1*. A Tukey post hoc test revealed that the Likelihood of Purchasing Smart Appliances was significantly lower in the Neutral Examples + Risk Examples condition (2.54 ± 1.29, $p = .047$) compared to the Neutral Examples condition (3.35 ± 1.1), but not in comparison to Traditional Content, Control or Traditional Content + Neutral Examples. No other comparisons were significant.

Table 3.4. Descriptive Statistics and Correlations for All Measures.

Variable	Mean	*SD*	1	2	3	4	5	6	7	8	9	10	11	12	13
1. T	-	-	-												
2. Control	-	-	-	-											
3. T + N	-	-	-	-	-										
4. N	-	-	-	-	-	-									
5. N + R	-	-	-	-	-	-	-								
6. LPSA	2.95	1.23	.052	.073	-.108	.130	-.146*	-							
7. CInfoMis	-	-	.014	.024	.077	-.200**	.118	-.348**	-						
8. ComUInfo	-	-	.011	.152*	.039	-.140	-.022	-.025	.422**	-					
9. CPerInfo	-	-	.019	.056	.045	-.096	.010	-.225**	.647**	.494**	-				
10. ContInfo	-	-	.131	-.041	-.106	.125	-.078	.440**	-.330**	-.016	-.329**	-			
11. HardTL	4.48	.57	-.032	-.131	.124	.050	-.012	.164*	.022	.079	.056	.074	-		
12. SocMedTL	4.26	.75	.031	-.006	.088	-.023	-.092	.145*	.079	.198**	.041	.160*	.494**	-	
13. SoftTL	4.22	.76	-.016	.032	.026	.107	-.162*	.078	.132	.106	.093	.042	.512**	.580**	-
14. CKnowTL	4.07	.76	.078	-.016	.084	.003	-.132	.157*	.054	.020	-.030	.161*	.481**	.357**	.475**

Note. N = 188

T = Traditional Content; T + N = Traditional Content + Neutral Examples; N = Neutral Examples; N + R = Neutral Examples+ Risk Examples; LPSA = Likelihood of Purchasing Smart Appliances; CInfoMis = Concern about Information Misuse; ComUInfo = Companies Should Not Use, Share, and Sell User Information; CPerInfo = Concern about Personal Information; ContInfo = Contact Information; HardTL = Hardware Technology Literacy; SocMedTL = Social Media Technology Literacy; SoftTL = Software Technology Literacy; CKnowTL = Comparative Knowledge Technology Literacy.

**p* < .05. ***p* < .01.

Second, to test H2 that technology literacy moderated the relationship between Abstractness of Privacy Disclosures and Privacy Attitudes, and H3 that Privacy Attitudes mediated the relationship between Abstractness of Privacy Disclosures and Privacy Behaviors, a moderated mediation was conducted using the PROCESS macro by Andrew F. Hayes (2018). Moderated mediation analyses determined the effects of the multiple mediator and moderator variables on the sharing of Contact Information in each condition of the Abstractness of Privacy Disclosures, as shown by the overall model (Figure 3.1.). The three mediator variables – Concern about Information Misuse (CInfoMis), Companies Should Not Use, Share, and Sell User Information (ComUInfo), and Concern about Personal Information (CPerInfo) – and four moderator variables – Hardware Technology Literacy, Social Media Technology Literacy, Software Technology Literacy, and Comparative Knowledge Technology Literacy – were paired with each other to create twelve models. Table 3.5. provides a brief overview of the variables used in each model.

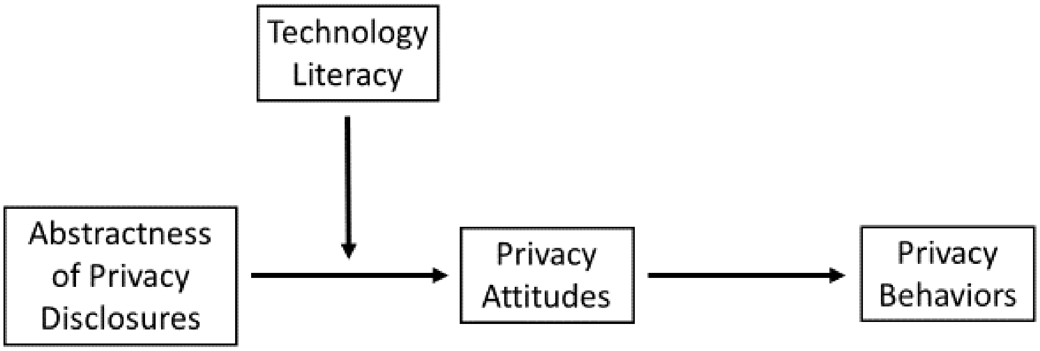

Figure 3.1. Overall Model.

Table 3.5. List of Variables for Each Model.

Model	IV	DV	Moderator	Mediator
1	APD	Contact Information	Hardware TL	CInfoMis
2	APD	Contact Information	Hardware TL	ComUInfo
3	APD	Contact Information	Hardware TL	CPerInfo
4	APD	Contact Information	Social Media TL	CInfoMis
5	APD	Contact Information	Social Media TL	ComUInfo
6	APD	Contact Information	Social Media TL	CPerInfo
7	APD	Contact Information	Software TL	CInfoMis
8	APD	Contact Information	Software TL	ComUInfo
9	APD	Contact Information	Software TL	CPerInfo
10	APD	Contact Information	Comparative Knowledge TL	CInfoMis
11	APD	Contact Information	Comparative Knowledge TL	ComUInfo
12	APD	Contact Information	Comparative Knowledge TL	CPerInfo

Note. APD = Abstractness of Privacy Disclosures; TL = Technology Literacy; CInfoMis = Concern about Information Misuse; ComUInfo = Companies Should Not Use, Share, and Sell User Information; CPerInfo = Concern about Personal Information.

From the 12 Models, only Model 1 and Model 4 revealed significant findings. The remaining ten models did not have any significant effects. The results of all 12 models are provided in Appendix I.

3.3.1. Model 1. From Table I.1., the moderated mediation analysis revealed that there was a significant interaction between the Traditional Content + Neutral Examples condition and Hardware Technology Literacy on Concern about Information Misuse (b = 1.02, p < .05, 95% CI = .2406 to 1.7969), in support of *H2*. Specifically, compared to participants in the Traditional Content condition (reference condition), when participants' Hardware Technology Literacy was high, those in the Traditional Content + Neutral Examples condition reported greater Concern about Information Misuse while those who were low in Hardware Technology Literacy reported less concern. Concern about Information Misuse had a significant effect on Contact Information (b = -.32, p < .001, 95% CI = -.4612 to -.1737). From Table I.2., it was noted that the index of moderated mediation was significant in the Traditional Content + Neutral Examples condition (*b* = -.32, *SE* = .16, 95% CI = -.6591 to -.0351). The conditional indirect effect (b = -.18, SE = .10, 95% CI = -.3801 to -.0013) suggests that there is a significant indirect effect of the condition Traditional Content + Neutral Examples on sharing Contact Information when participants' Hardware Technology Literacy is high, in support of *H3*. Overall, the negative indirect effect of Traditional Content + Neutral Examples on sharing Contact Information when Hardware Technology Literacy is high suggests that when participants read the Traditional Content with Neutral Examples and have high Hardware Technology Literacy, they are less likely to share Contact Information because they have greater Concern about Information Misuse.

3.3.2. Model 4. From Table I.7., the moderated mediation analysis revealed that there was a significant interaction between Traditional Content + Neutral Examples and Social Media Technology Literacy on Concern about Information Misuse, (*b* = .73, *p* < .05, 95% CI = .1075 to 1.3551), in support of *H2*. There was also a significant interaction between Neutral Examples and Social Media Technology Literacy on Concern about Information Misuse (*b* = .58, *p* < .05, 95% CI = .0046 to 1.1495), also in support of *H2*. Specifically, compared to participants in the Traditional Content condition, when participants' Social Media Technology Literacy was high, those in the Traditional Content + Neutral Examples and Neutral Examples conditions reported greater Concern about Information Misuse while those who were low in Social Media Technology Literacy reported less concern. Concern about Information Misuse had a significant effect on Contact Information (*b* = -.35, *p* < .001, 95% CI = -.4949 to -.2061). From Table I.8., it was noted that the index of moderated mediation was significant in the Neutral Examples condition (*b* = -.20, *SE* = .11, 95% CI = -.4588 to -.0254). The conditional indirect effect (*b* = .33, *SE* = .13, 95% CI = .1286 to .6355) suggests that there is a significant indirect effect of the condition Neutral Examples on sharing Contact Information when the participants' Social Media Technology Literacy was low, in support of *H3*. Overall, the positive indirect effect of Neutral Examples on sharing Contact Information when Social Media Technology Literacy is low suggests that when participants read the Neutral Examples and are low in Social Media Technology Literacy, they are more likely to share their Contact Information because they have a lower Concern about Information Misuse. While there was a significant index of moderated mediation in the Traditional Content + Neutral Examples condition (*b* = -.26, *SE* = .13, 95% CI = -.5326 to -.0311), there were no significant conditional indirect effects (low Social Media Technology Literacy, *b* = .18, *SE = .13*, 95% CI = -.0503 to .4558; high Social Media Technology Literacy, *b* = -.21, *SE* = .12, 95% CI = -.4523 to 0165).

3.3.3. Conditional Direct Effects. Table 3.6. includes the conditional direct effects of all 12 models. The participants who were in conditions of Traditional Content + Neutral Examples and Neutral Examples + Risk Examples, and were high in technology literacy (hardware, social media, software, and comparative knowledge) were less likely to share their Contact Information as indicated by the negative direct effects. Participants were less likely to share Contact Information when they read the Traditional Content + Neutral Examples condition or Neutral Examples + Risk Examples condition and had a high technology literacy of any kind, regardless of the privacy attitudes in the respective models. Therefore, having a high technology literacy appears to be helpful to participants to help them understand the policy information particularly when Neutral Examples were combined with Traditional Content or Risk Examples, respectively.

Table 3.6. Conditional Direct Effects.

	Condition	Moderator	*b* (*SE*)
Model 1	Control	Low Hardware TL	-.40 (.24)
	Control	High Hardware TL	-.11 (.29)
	Traditional + Neutral	Low Hardware TL	-.22 (.30)
	Traditional + Neutral	High Hardware TL	-.60 (.27)*
	Neutral	Low Hardware TL	-.13 (.29)
	Neutral	High Hardware TL	-.14 (.28)
	Neutral + Risk	Low Hardware TL	-.11 (.28)
	Neutral + Risk	High Hardware TL	-.66 (.30)*
Model 2	Control	Low Hardware TL	-.37 (.26)
	Control	High Hardware TL	-.16 (.31)
	Traditional + Neutral	Low Hardware TL	-.08 (.31)
	Traditional + Neutral	High Hardware TL	-.78 (.29)*
	Neutral	Low Hardware TL	.06 (.30)
	Neutral	High Hardware TL	-.05 (.30)
	Neutral + Risk	Low Hardware TL	-.11 (.29)
	Neutral + Risk	High Hardware TL	-.78 (.32)*
Model 3	Control	Low Hardware TL	-.36 (.24)
	Control	High Hardware TL	-.11 (.29)
	Traditional + Neutral	Low Hardware TL	-.14 (.29)
	Traditional + Neutral	High Hardware TL	-.67 (.27)*
	Neutral	Low Hardware TL	-.04 (.29)
	Neutral	High Hardware TL	-.15 (.28)
	Neutral + Risk	Low Hardware TL	-.15 (.27)
	Neutral + Risk	High Hardware TL	-.73 (.30)*
Model 4	Control	Low Social Media TL	-.41 (.29)
	Control	High Social Media TL	-.20 (.28)
	Traditional + Neutral	Low Social Media TL	-.22 (.33)
	Traditional + Neutral	High Social Media TL	-.58 (.28)*
	Neutral	Low Social Media TL	-.18 (.32)
	Neutral	High Social Media TL	-.11 (.29)
	Neutral + Risk	Low Social Media TL	.03 (.29)
	Neutral + Risk	High Social Media TL	-.66 (.30)*
Model 5	Control	Low Social Media TL	-.28 (.31)
	Control	High Social Media TL	-.31 (.30)
	Traditional + Neutral	Low Social Media TL	-.05 (.35)
	Traditional + Neutral	High Social Media TL	-.78 (.30)*

Table 3.6. Conditional Direct Effects (cont.).

	Condition	Moderator	*b* (*SE*)
	Neutral	Low Social Media TL	.13 (.33)
	Neutral	High Social Media TL	-.10 (.31)
	Neutral + Risk	Low Social Media TL	-.01 (.31)
	Neutral + Risk	High Social Media TL	-.72 (.32)*
Model 6	Control	Low Social Media TL	-.25 (.29)
	Control	High Social Media TL	-.31 (.28)
	Traditional + Neutral	Low Social Media TL	-.10 (.33)
	Traditional + Neutral	High Social Media TL	-.67 (.28)*
	Neutral	Low Social Media TL	-.03 (.31)
	Neutral	High Social Media TL	-.14 (.29)
	Neutral + Risk	Low Social Media TL	.03 (.29)
	Neutral + Risk	High Social Media TL	-.74 (.30)*
Model 7	Control	Low Software TL	-.61 (.28)*
	Control	High Software TL	-.07 (.28)
	Traditional + Neutral	Low Software TL	-.30 (.30)
	Traditional + Neutral	High Software TL	-.52 (.30)
	Neutral	Low Software TL	-.39 (.32)
	Neutral	High Software TL	.04 (.29)
	Neutral + Risk	Low Software TL	-.18 (.25)
	Neutral + Risk	High Software TL	-.65 (.32)*
Model 8	Control	Low Software TL	-.51 (.30)
	Control	High Software TL	-.16 (.30)
	Traditional + Neutral	Low Software TL	-.22 (.32)
	Traditional + Neutral	High Software TL	-.69 (.32)*
	Neutral	Low Software TL	-.04 (.34)
	Neutral	High Software TL	.06 (.31)
	Neutral + Risk	Low Software TL	-.25 (.27)
	Neutral + Risk	High Software TL	-.72 (.35)*
Model 9	Control	Low Software TL	-.48 (.28)
	Control	High Software TL	-.15 (.28)
	Traditional + Neutral	Low Software TL	-.23 (.30)
	Traditional + Neutral	High Software TL	-.60 (.30)*
	Neutral	Low Software TL	-.34 (.32)
	Neutral	High Software TL	.09 (.29)
	Neutral + Risk	Low Software TL	-.24 (.25)
	Neutral + Risk	High Software TL	-.73 (.33)*
Model 10	Control	Low CompKnow TL	-.40 (.29)
	Control	High CompKnow TL	.02 (.34)
	Traditional + Neutral	Low CompKnow TL	-.26 (.29)
	Traditional + Neutral	High CompKnow TL	-.59 (.31)
	Neutral	Low CompKnow TL	-.18 (.32)
	Neutral	High CompKnow TL	-.03 (.34)
	Neutral + Risk	Low CompKnow TL	-.11 (.27)
	Neutral + Risk	High CompKnow TL	-.71 (.35)*

Table 3.6. Conditional Direct Effects (cont.).

	Condition	Moderator	*b* (*SE*)
Model 11	Control	Low CompKnow TL	-.32 (.31)
	Control	High CompKnow TL	-.08 (.36)
	Traditional + Neutral	Low CompKnow TL	-.19 (.30)
	Traditional + Neutral	High CompKnow TL	-.75 (.33)*
	Neutral	Low CompKnow TL	.08 (.33)
	Neutral	High CompKnow TL	-.02 (.37)
	Neutral + Risk	Low CompKnow TL	-.09 (.29)
	Neutral + Risk	High CompKnow TL	-.87 (.38)*
Model 12	Control	Low CompKnow TL	-.37 (.29)
	Control	High CompKnow TL	.03 (.34)
	Traditional + Neutral	Low CompKnow TL	-.23 (.28)
	Traditional + Neutral	High CompKnow TL	-.62 (.31)*
	Neutral	Low CompKnow TL	-.15 (.32)
	Neutral	High CompKnow TL	.03 (.34)
	Neutral + Risk	Low CompKnow TL	-.12 (.27)
	Neutral + Risk	High CompKnow TL	-.87 (.35)*

Note. TL = Technology Literacy; CompKnow = Comparative Knowledge
*p < .05. **p < .01. ***p < .001

4. DISCUSSION

In this study, new scales were developed for measuring smart appliance privacy behaviors and technology literacy. The Privacy Attitudes questionnaire captured dimensions of Concern about Information Misuse, Companies and Users Do Not Devote Time and Resources for User Protection, Companies Should Not Use, Share, and Sell User Information, and Concern about Personal Information. The Privacy Behaviors questionnaire captured dimensions of sharing Contact Information, sharing Purchase History, sharing Date of Birth, and sharing Financial Information. Based on how these items grouped together in the factor analyses, it is possible that sharing behaviors are the same across the three different contexts of online shopping, membership and rewards programs, and warranty and product support. For example, when participants are willing to share their Contact Information such as Name in one context, they are willing to share it in the other two contexts as well.

Participants in the Neutral Examples condition were most likely to purchase smart appliances compared to those in the Neutral Examples + Risk Examples condition who were least likely to purchase smart appliances. These conditions were significantly different from each other. It may be that once participants were aware of the risks associated with smart appliances in the form of examples, they were able to understand how their privacy could be affected, as opposed to those participants who only received examples about the features or benefits of the smart appliances. It is possible that the participants in the Neutral Examples + Risk Examples condition engaged in a benefit analysis and concluded that the benefits do not outweigh the risks attached. Therefore, the examples provided were utilized to guide the decision making process. It should be noted that the Neutral Examples group did have access to the legal privacy policy that stated the risks. However, it is likely that, even if the legal verbiage was expanded, this particular privacy policy condition did not allow for the risks associated with the Neutral Examples to be ascertained efficiently.

Participants in the Traditional Content + Neutral Examples condition who had high Hardware Technology Literacy, had an increased Concern about Information Misuse, and were less likely to share their Contact Information. It is possible that participants with high Hardware Technology Literacy were able to understand the legal verbiage in conjunction with the Neutral Examples provided due to their experience with technology. Therefore, they were able to utilize the Neutral Examples and Traditional Content to understand how their privacy could be affected, leading to higher privacy attitudes, and reduced Contact Information sharing. Participants in the Neutral Examples condition who had low Social Media Technology Literacy, had a decreased Concern about Information Misuse, and were more likely to share their Contact Information. It is possible that participants with low Social Media Technology Literacy were not able to understand the risks associated with information sharing in a Neutral Examples context alone. Therefore, they have lower privacy attitudes and increased Contact Information sharing. Additionally, participants in the Traditional Content + Neutral Examples and Neutral Examples + Risk Examples conditions who had high technology literacy were less likely to share their Contact Information, irrespective of their privacy attitudes. It is possible that participants with high technology literacy of any kind made privacy conscious decisions because they were able to use the information provided to them in the form of a Neutral Examples component coupled with Traditional Content and Risk Examples, respectively.

It is important to consider the matter with individuals who have low technology literacy. As the matter stands, it appears that individuals with lower technology literacy, regardless of condition, are unable to grasp how their privacy is potentially affected by new technology and therefore do not have an increased concern for privacy. Arguably, as technology continues to improve and evolve, there will always be a group of individuals with more experience to utilize that piece of technology effectively and efficiently. At the same time, there will also be a group of individuals with less experience who are unable to use that technology efficiently. As time progresses, there is a possibility that the individuals with low technology literacy increase their technology literacy. However, there is a strong likelihood that a new piece of technology will be produced and introduced in the market, resulting in groups of high technology literate individuals and low technology literate individuals once again. It is important to note the possibility that individuals with low technology literacy will not always remain low. Nevertheless, there is a distinct possibility that a new group of individuals with low technology literacy will emerge. It is essential to create methods to help individuals with low technology literacy. Eye tracking software can be utilized to measure whether individuals are paying attention to the privacy policy information provided to them. If it is being read, then the next logical step is to find methods to improve technology literacy either through online workshops or through tutorials. If the privacy policy is not being read, then it will be critical to understand why individuals with low technology literacy are ignoring the policy information.

5. LIMITATIONS AND FUTURE RESEARCH

There are several limitations that need to be discussed. First, the amount of materials the participants had to read through was significant. While the privacy policy content in this experiment was much shorter than the conventional policies currently used, previous research suggests people do not read policies in their entirety. Therefore, it cannot be said with complete surety that participants read the entire privacy policy they were presented with. In the future, determining whether the policy provided was read completely would be helpful.

Second, it is possible that the participants' privacy attitudes and privacy behaviors regarding smart appliances were formed as a result of reading their respective privacy policy condition and their current levels of technology literacy. However, the participants' privacy attitudes and behaviors without the privacy policy content and components were not determined. In the future, it would be of interest to measure the participants' privacy attitudes and behaviors prior to the introduction of privacy policy content and components in one survey, followed by an invite to participate in a second measurement of their attitudes and behaviors after introducing the privacy policy content and components to determine if there were any changes.

Third, this cross-sectional research primarily provides a snapshot in time regarding how individuals utilize the components of information provided in privacy policies to form their privacy attitudes and behaviors. Study data was collected prior to news reports about use of data collected from social media platforms. With the recent focus on privacy in the news regarding social media and updated online privacy policies, it is possible that individuals are now more aware of how their data is collected and used. Therefore, it will be interesting to conduct the experiment again to analyze if there were any changes regarding privacy attitudes and behaviors.

Finally, there were several variables that were excluded from the analysis. This was done to reduce the number of models that would need to be run due to time constraints for this current project. Additionally, having many combinations would not have been appropriate, as effects may have been significant by chance alone if all possible models were analyzed. It would be of interest to complete the remaining analysis to determine if the remaining variables shed light on understanding privacy attitudes and behaviors. The findings of the current study need to be replicated. However, it is suggested that future studies to replicate findings be conducted on a model-by-model basis.

6. CONCLUSION

The results of this study are a step in the right direction to help people focus on thinking about the entire smart home concept before people start residing in smart homes. Comparing different components of Traditional Content, Neutral Examples, and Risk Examples provided an understanding of how individuals utilized the information provided. It is possible that certain combinations of the components provided information to reduce the abstractness surrounding privacy policies, which led to alignment of attitudes and behaviors. The results of this study make an argument that privacy policies should include concrete examples, such as Neutral Examples, to explain the legal verbiage in each section. Introducing neutral examples can be a starting point so individuals can understand the technical and legal language in lay terms. The study also makes a case that if privacy policies remain as they are, then they are possibly the least effective way of providing individuals with information to facilitate consistency.

Additionally, it is important to consider individuals' technology literacy as they read privacy policies because it played a key role in the affecting the relationships between the variables of this study. It is suggested that efforts should be made to increase the technology literacy of consumers so they can understand privacy policies and are able to align their privacy attitudes with behaviors. It is important to equip people with the right knowledge prior to the time for fully automated living, so that when the time comes people make well-informed decisions regarding privacy that can hopefully prevent actual privacy violations. Therefore, it is important to focus on creating privacy policies that utilize examples and develop technology literacy in order to enable people to understand the policies they read and make appropriate choices regarding privacy.

APPENDIX A.

TRADITIONAL CONTENT

Introducing the Smartenna Product Line

Smartenna has created a collection of internet-connected appliances and technologies that make the home convenient. This collection includes refrigerators, dishwashers, washing machines, dryers, thermostats, etc. Smartenna appliances offer features such as connections to social networks, customized content, service and product recommendations, and supported applications. These features can be customized based on the owner's interactions with the appliance. Smartenna appliances improve user experience and provide ease of access for many goods and services. To improve functionality of these appliances owner data is collected, used, stored, shared, and protected through each appliance in the ways described by the Smartenna Privacy Policy. The policy describes the practices related to this new collection of smart appliances. Please take time to read this Privacy Policy found below.

Smartenna Privacy Policy and Disclosure Statement

Section 1. Background

Smartenna appliances communicate with one another via WIFI, but do not need to be connected to the internet to function. However, many of the advanced features of Smartenna products require they be connected to the internet. When connected to the internet Smartenna collects information about how each appliance is used by the owner. This information may include, but is not limited to, products that have been viewed, purchased or watched, search terms, reviews, likes or dislikes through various Smartenna appliances. If internet connection is enabled, transmitted information will be used to provide customized content that is relevant to each appliance.

Section 2. Data Sharing Features

Each Smartenna appliance comes equipped with a range of features that require data sharing with Smartenna in order to function properly.

2.1. Connected Appliances

All Smartenna appliances can be connected to each other using WiFi and the Smartenna appliance software application. This application can be downloaded on a smartphone and can be activated by setting up a unique username and password. The owner can access, control, and monitor the appliance using the smartphone application. By using the application, the owner can be notified about appliance statuses. Once Smartenna appliances are connected to the smartphone application, data gathered by one appliance can be made available on another appliance. Additional information such as alerts, event data, idle time, number of times the appliance is turned on or off, past purchases, and diagnostic information are collected and stored. Appliances connecting via the Smartenna application may still be controlled manually.

2.2. Voice Recognition

By enabling Voice Recognition on a Smartenna appliance, regular speech can be used to control many functions of that appliance. In order to provide this Voice Recognition feature, any voice sounds detected by the Smartenna microphone are transmitted to third party services to convert this data to text and search for relevant commands and requests. Appliance information and related identifiers are also transmitted. This information may also be used by Smartenna to evaluate and improve features of the appliance. When this feature is disabled, the appliance can be operated using remote controls or touchpad depending on the type of appliance.

Section 3. Social Media and Appliances

All Smartenna products in this new collection can be connected to social media. The owner is in control of allowing which appliances connect with online platforms. When using social networking applications on a Smartenna appliance, any information provided will be subject to the social media platform settings that are set up with that provider. Smartenna will make metadata available such as the time of posts and the appliance used to share the information. Smartenna may have reciprocal contracts with online platforms to access information such as name, biography, location, and pictures provided on the account. This information may be analyzed for trends and generates insight on customers. It is advised that customers review social media settings and appliance settings to control who has access to this information and how it is used.

By accessing and using Smartenna products and services, you agree to accept the terms and conditions of this Privacy Policy. You will gain access to the latest smart technology that is on the market which enables you to perform multiple tasks using one appliance. We will use your information according to the latest version of the Privacy Policy. As Smartenna continues to grow and change, we will make updates to this Privacy Policy. You are advised to check back and review these changes on a periodic basis. For any significant change, we will make prominent announcements such as a message on your appliance’s screen or through email.

APPENDIX B.

NEUTRAL EXAMPLES

2.1. Connected Appliances: How it works.

Aaron has several smart appliances connected to his smartphone Smartenna application. He uses customized settings on his connected appliances to save energy and money. Aaron hires Susan to house sit for a short period of time during summer vacation. He authorizes Susan’s smartphone so she can control the smart appliances while he is away. Susan can see how Aaron operates his appliances so that she can operate them the same way while he is gone to continue his energy savings plan – including washer/dryer cycles settings, dishwasher settings and usage times, ordering product refills, etc.

2.2. Voice Recognition: How it works.

Janice’s smart refrigerator has the Smartenna Voice Recognition feature enabled. Since this feature is enabled, Janice's refrigerator continually records and transmits conversations she has even when she is not directing those conversations to the refrigerator. These recordings are transmitted to a data collection center where they may be transcribed and stored in a database and used to control the function of the appliance. For example, she uses this feature while meal planning for the week. She can decide if she has all the items to cook her recipes, using voice command to ask the refrigerator to list the food items within it. This reduces the number of times she opens the refrigerator to look at its contents which saves energy and time.

Section 3. Social Media and Appliances: How it works.

Casey has her refrigerator, washer, and television connected to her social media account and likes to make posts using her appliances as she goes about her daily activities. Casey is utilizing a streaming service to watch movies and shows on her

Smartenna connected television, which she has connected to her social media account. When she watches a movie or program, the television prompts her to post an update. When Casey approves these posts a status update is posted to her social media account letting people know what she is watching.

APPENDIX C.

RISK EXAMPLES

2.1. Connected Appliances: Example of potential risk.

About 10 months later, Susan messages Aaron that she is available to house-sit over the summer again and sends him a gift basket containing his favorite coffee brand, specialty coffee creamers, and nutrition bars. Aaron is certain he didn’t mention these favorite items to Susan, and when he asks about it she mentions that while she house-sat, she noticed he had purchased these products in the past via the Smartenna application history for his fridge and coffee maker.

2.2. Voice Recognition: Example of potential risk.

Janice receives coupons in the mail for party supplies, a bouncy house and children’s toys. She is confused as to why she received coupons specifically addressed to her. She realizes she had a conversation with her parents about her youngest brother’s birthday party while she was meal prepping a few days ago. They had discussed the party plans and she explained how coupons could be used to get certain items at a discounted price. A third party company sent her coupons based on the party planning conversation that her refrigerator recorded due to the Voice Recognition feature.

Section 3. Social Media and Appliances: Example of potential risk.

Casey’s television posted a status that she was watching her favorite television show “Bake Wars.” Casey’s friend Ruth noticed on social media what Casey is currently watching so Ruth decides to surprise Casey by going to her house, so they can watch the show together. Ruth knew Casey was at home because the status updates posted ‘via Smartenna Television’ at the bottom of each post.

APPENDIX D.

DISTRACTION TASK

Items 1, 4, and 6 are measured using a 5 point Likert Scale (1=Strongly Disagree, 5=Strongly Agree)

Smart appliances are appliances that connect to your smartphone or computer, and provide you with controls to manage appliances from wherever you are. These connections are made using Wi-Fi and have a variety of settings that can be customized to the owner's needs.

Example 1: A smart oven can be switched on and preheated to a desired temperature directly from your smartphone. You do not have to enter the kitchen to set it up.

Example 2: A smart refrigerator could be equipped with an internal camera that allows you to view the contents of your refrigerator while you are out shopping for groceries.

1. I am likely to purchase smart appliances.

2. If you were to purchase a smart appliance, which one(s) would you like to purchase?

Select *ALL* that apply.

○ Smart Oven – control oven temperature for preheating, on/ off features, and cooking with a smartphone.

○ Smart Refrigerator – equipped with an internal camera to view contents.

○ Smart Dishwasher – informs you when detergent levels are low and orders directly from store or preferred vendor.

○ Smart Washer – control washer cycle and settings with your smartphone.

○ Smart Dryer – receive signal from washer to automatically use appropriate drying cycle.

○ Smart Lights – control brightness and on/off features with your smartphone or voice command.

○ Smart TV – search for and play movies or television shows using voice command.

○ Smart Thermostat – control temperature settings using your phone or voice command.

○ Smart Coffee Maker – brew your daily cup of coffee using your smartphone.

3. List any other smart appliances you would like to purchase. *(open entry)*

4. The following smart appliance features are appealing to me.

4a. Energy Savings

4b. Diagnosing problems for warranty coverage

4c. Communication between appliances

4d. Voice Recognition

4e. Remote Monitoring

5. List any other features that would be appealing to you. *(open entry)*

6. The following aspects of smart appliances to are important to me.

6a. Easy to Use

6b. Price

6c. Design

6d. Device Interface

6e. Brand

7. List any other aspects that would be appealing to you. *(open entry)*

APPENDIX E.

PRIVACY ATTITUDES QUESTIONNAIRE

The following items are measured using a 5 point Likert Scale (1=Strongly Disagree, 5=Strongly Agree)

1. Generally speaking, it bothers me when websites ask me for personal information.

2. Generally speaking, when websites ask me for personal information, I think twice before providing it.

3. Generally speaking, I am concerned that websites are collecting personal information about me.

4. Companies and manufacturers of smart appliances devote appropriate resources (such as time, money, effort) to protecting my personal information.

5. Users devote appropriate resources towards preventing illegal access to personal information on smart appliances (such as reading policies, changing passwords, customizing privacy settings).

6. Databases that contain personal information collected from smart appliances should be protected from illegal access – no matter how much it costs.

7. Companies and manufacturers take steps to make sure that hackers cannot access the personal information in their smart appliances.

8. Users take steps to make sure that hackers cannot access the personal information in their smart-appliances.

9. Smart appliance companies should not use personal information for purposes that have not been authorized by the individual who provides the information.

10. The company can use the personal information provided by smart appliance users for any reason.

11. Company databases should never sell the personal information they have collected from smart appliances to third party vendors.

12. Smart appliance companies should never share personal information with other websites or companies unless it has been authorized by the individuals who provided the information.

13. I am concerned that the information I submit to the smart appliance could be misused.

14. I am concerned that a person can find private information about me because of a smart appliance.

15. I am concerned about submitting information on the smart appliance because of what others might do with it.

16. I am concerned about submitting information on a smart appliance because it could be used in a way I did not foresee.

Reverse Scored Items: 4, 5, 7, 8

APPENDIX F.

PRIVACY BEHAVIORS QUESTIONNAIRE

Items 1, 7, 8, and 9 are measured using a 5 point Likert Scale (1=Strongly Disagree, 5=Strongly Agree)

Items 2, 3, 4, 5 and 16 are measured using a dichotomous variable (Yes, No)

Items 2a-2h, 3a-3h, and 4a-4h are measured using a 5 point Likert Scale (1=Never, 5=Always)

Items 11b, 12b, 13b, and 14b are measured using a 5 point Likert Scale (1=Extremely Likely to Decrease privacy settings, 5=Extremely Likely to Increase privacy settings)

Items 15 and 17 are measured using a trichotomous variable (Yes, No, I don't know)

1. When shopping for smart appliances, I am likely to provide the vendor with my personal information needed to better serve my needs.

Online Shopping

2. When shopping online, I am willing to share the following information about myself:

a. Name

b. Date of Birth

c. Email

d. Home Address

e. Phone Number

f. Social Security Number

g. Past Purchasing Information from other vendors

h. Income

2a. You indicated you are willing to share your *Name*, how often are you willing to share it?

2b. You indicated you are willing to share your *Date of Birth*, how often are you willing to share it?

2c. You indicated you are willing to share your *Email*, how often are you willing to share it?

2d. You indicated you are willing to share your *Home Address*, how often are you willing to share it?

2e. You indicated you are willing to share your *Phone Number*, how often are you willing to share it?

2f. You indicated you are willing to share your *Social Security Number,* how often are you willing to share it?

2g. You indicated you are willing to share your *Past Purchasing Information*, how often are you willing to share it?

2h. You indicated you are willing to share your *Income,* how often are you willing to share it?

<u>Membership and Rewards Programs</u>

3. When signing up for smart appliance membership (rewards) programs, I am willing to share the following information about myself:

a. Name

b. Date of Birth

c. Email

d. Home Address

e. Phone Number

f. Social Security Number

g. Past Purchasing Information from other vendors

h. Income

3a. You indicated you are willing to share your *Name*, how often are you willing to share it?

3b. You indicated you are willing to share your *Date of Birth*, how often are you willing to share it?

3c. You indicated you are willing to share your *Email*, how often are you willing to share it?

3d. You indicated you are willing to share your *Home Address,* how often are you willing to share it?

3e. You indicated you are willing to share your *Phone Number*, how often are you willing to share it?

3f. You indicated you are willing to share your *Social Security Number*, how often are you willing to share it?

3g. You indicated you are willing to share your *Past Purchasing Information*, how often are you willing to share it?

3h. You indicated you are willing to share your *Income*, how often are you willing to share it?

<u>Warranty and Product Support</u>

4. When filling out information for warranty and product support for smart appliances, I am willing to share the following information about myself:

a. Name

b. Date of Birth

c. Email

d. Home Address

e. Phone Number

f. Social Security Number

g. Past Purchasing Information from other vendors

h. Income

4a. You indicated you are willing to share your *Name*, how often are you willing to share it?

4b. You indicated you are willing to share your *Date of Birth*, how often are you willing to share it?

4c. You indicated you are willing to share your *Email*, how often are you willing to share it?

4d. You indicated you are willing to share your *Home Address*, how often are you willing to share it?

4e. You indicated you are willing to share your *Phone Number*, how often are you willing to share it?

4f. You indicated you are willing to share your *Social Security Number*, how often are you willing to share it?

4g. You indicated you are willing to share your *Past Purchasing Information*, how often are you willing to share it?

4h. You indicated you are willing to share your *Income*, how often are you willing to share it?

<u>Social Media</u>

5. Do you have a social media account?

6. What is the primary reason(s) you don’t have social media? *(open entry)*

7. I am likely to post on social media.

8. I am likely to post status updates on social media.

9. I am likely to check in and post your location on social media.

10. Which of the following social media platforms do you use?

○ Facebook ○ Twitter ○ Snapchat ○ Instagram

11a. Thinking about my Facebook account, in the past I generally set my privacy settings to enable

○ Public ○ Friends ○ Friends of friends ○ Private (“Only Me”) ○ Custom (Block certain users)

11b. How likely are you to change your privacy settings?

12a. Thinking about my Twitter account, in the past I generally set my privacy settings to enable

○ Default ○ Approved audience (“Protect my Tweets”)

12b. How likely are you to change your privacy settings?

13a. Thinking about my Snapchat account, in the past I generally set my privacy settings to enable

○ Everyone ○ Friends ○ Custom (Choose specific friends)

13b. How likely are you to change your privacy settings?

14a. Thinking about my Instagram account, in the past I generally set my privacy settings to enable

○ Default ○ Approved audience (Private Account enabled)

14b. How likely are you to change your privacy settings?

Tagged: My name or social profile was linked to an image or post.

15. I have been tagged in a social media post without my approval.

16. Did you change your privacy settings after you were tagged in a social media post without your approval?

17. You indicated you did not know whether you were tagged in a social media post. Do you have any settings in place to prevent this from happening?

APPENDIX G.

TECHNOLOGY LITERACY QUESTIONNAIRE

The following items are measured using a 5 point Likert Scale (1=Strongly Disagree, 5=Strongly Agree, 0=Don't Know)

1. I find it easy to
   a. Use Smartphones
   b. Use Computers
   c. Use Laptops
   d. Use Tablets
   e. Navigate a new gaming platform (such as Xbox, PlayStation, Nintendo Wii) even if I haven't tried it before.
2. I find it easy to use
   a. Facebook
   b. Twitter
   c. Snapchat
   d. Instagram

3. I find it easy to use

   a. Email platforms (such as Google, Yahoo, Outlook, Hotmail)
   b. Word Processor (such as Microsoft Word, Google Docs)
   c. Presentation Software (such as Microsoft PowerPoint, Google Slides)
   d. Spreadsheet Software (such as Microsoft Excel, Google Sheets)
   e. Databased Management Systems (such as Microsoft Access, Oracle)
   f. Note Taking Software (such as Microsoft OneNote, Evernote)

4. Which of these programs do you believe offer password protection? Select all that apply.

○ Email platforms (such as Google, Yahoo, Outlook, Hotmail)

○ Word Processor (such as Microsoft Word, Google Docs)

○ Presentation Software (such as Microsoft PowerPoint, Google Slides)

○ Spreadsheet Software (such as Microsoft Excel, Google Sheets)

○ Database Management Systems (such as Microsoft Access, Oracle)

○ Note taking Software (such as Microsoft OneNote, Evernote)

5. I am technology savvy

a. Compared to my friends.
b. Compared to my coworkers.
c. Compared to my family members.
d. Compared to the general public

6. I get frustrated navigating through

a. Social Media when I want to make a post.
b. Smartphones when trying to do basic tasks like phone calls, text messages and emails.
c. My computer to access files I’ve saved.
d. My computer to back up my drive.
e. My computer to organize my files.

APPENDIX H.

DEMOGRAPHICS

1. Please enter your age. *(open entry box)*
2. Please select your gender. (Male, Female, Other – *open entry*).
3. Please select the highest level of education you have completed. You may select more than one option, if applicable.
    a. GED
    b. High school diploma
    c. Associate’s degree (2-year program)
    d. Bachelor’s degree (4-year program)
    e. Master’s degree
    f. PhD or Professional Degree (MD, PharmD, DDS, DPT, JD)
    g. Technical Training
    h. Certification

   If 2G or 2H are selected, then ask question 3

4. You indicated you have received some kind of technical training or certification, please enter the type of training (for example, information technology, electronics, ventilation, etc.) *(open entry)*
5. Please enter your educational background or current field of study. *(open entry)*
6. Please enter your occupation or field of work. *(open entry)*
7. How many years of professional work experience do you have? *(open entry)*

APPENDIX I.

MODERATED MEDIATION ANALSYSIS – 12 MODELS

Table I.1. Model 1 – Overall Model Using Hardware Technology Literacy as Moderator and Concern About Information Misuse as Mediator.

	DV1 = CInfoMis	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	1.09 (1.06)	-.71 (1.01)
CInfoMis		-.32 (.07)***
Control	-1.07 (1.56)	-1.54 (1.48)
T+N	-4.53 (1.81)*	1.26 (1.75)
N	-1.97 (1.70)	-.09 (1.62)
N+R	-1.47 (1.84)	2.07 (1.75)
HardTL	-.24 (.24)	.22 (.22)
Control × HardTL	.25 (.35)	.28 (.34)
T+N × HardTL	1.02 (.39)*	-.37 (.38)
N × HardTL	.34 (.37)	-.01 (.35)
N+R × HardTL	.37 (.41)	-.55 (.39)
R^2	.09	.18***

Note. N = 180

CInfoMis = Concern about Information Misuse; ContInfo = Contact Information; HardTL = Hardware Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.2. Model 1 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low HardTL	.03 (.07)	(-.13, .17)		
Control/ High HardTL	-.05 (.11)	(-.25, .18)	-.08 (.11)	(-.29, .16)
T+N/ Low HardTL	.15 (.13)	(-.10, .42)		
T+N/ High HardTL	-.18 (.10)	**(-.38, -.0013)**	-.32 (.16)	**(-.66, -.04)**
N/ Low HardTL	.20 (.11)	**(.03, .44)**		
N/ High HardTL	.09 (.10)	(-.12, .28)	-.11 (.13)	(-.39, .11)
N+R/ Low HardTL	-.00 (.09)	(-.19, .17)		
N+R/ High HardTL	-.12 (.10)	(-.33, .07)	-.12 (.13)	(-.37, .13)

Note. N = 180

HardTL = Hardware Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

Table I.3. Model 2 – Overall Model Using Hardware Technology Literacy as Moderator and Companies Should Not Use, Share, and Sell User Information as Mediator.

	DV1 = ComUInfo	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	-.56 (.99)	-1.06 (1.06)
ComUInfo		-.00 (.08)
Control	.07 (1.46)	-1.19 (1.56)
T+N	-3.09 (1.70)	2.70 (1.83)
N	.39 (1.59)	.54 (1.70)
N+R	.40 (1.72)	2.53 (1.84)
HardTL	.14 (.22)	.30 (.24)
Control × HardTL	.03 (.33)	.21 (.35)
T+N × HardTL	.67 (.37)	-.69 (.40)
N × HardTL	-.18 (.35)	-.12 (.37)
N+R × HardTL	-.12 (.39)	-.66 (.41)
R^2	.09	.09

Note. N = 180

ComUInfo = Companies Should Not Use, Share, and Sell User Information; ContInfo = Contact Information; HardTL = Hardware Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.4. Model 2 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low HardTL	-.0003 (.03)	(-.05, .06)		
Control/ High HardTL	-.0003 (.02)	(-.05, .05)	.0000 (.02)	(-.06, .05)
T+N/ Low HardTL	.0006 (.04)	(-.09, .09)		
T+N/ High HardTL	-.0003 (.02)	(-.06, .05)	-.0009 (.06)	(-.12, .12)
N/ Low HardTL	.0004 (.04)	(-.10, .07)		
N/ High HardTL	.0007 (.05)	(-.10, .10)	.0002 (.04)	(-.07, .10)
N+R/ Low HardTL	.0001 (.02)	(-.05, .05)		
N+R/ High HardTL	.0002 (.03)	(-.06, .06)	.0002 (.03)	(-.07, .07)

Note. N = 180

HardTL = Hardware Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

Table I.5. Model 3 – Overall Model Using Hardware Technology Literacy as Moderator and Concern About Personal Information as Mediator.

	DV1 = CPerInfo	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	.02 (1.04)	-1.05 (1.00)
CPerInfo		-.34 (.07)***
Control	-.45 (1.53)	-1.35 (1.47)
T+N	-2.19 (1.77)	1.94 (1.71)
N	-.36 (1.67)	.41 (1.60)
N+R	-1.16 (1.80)	2.14 (1.73)
HardTL	.0028 (.23)	.30 (.22)
Control × HardTL	.12 (.35)	.25 (.33)
T+N × HardTL	.50 (.39)	-.52 (.37)
N × HardTL	.01 (.37)	-.11 (.35)
N+R × HardTL	.26 (.40)	-.57 (.39)
R^2	.04	.20***

Note. N = 180

CPerInfo = Concern about Personal Information; ContInfo = Contact Information; HardTL = Hardware Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.6. Model 3 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low HardTL	-.01 (.09)	(-.21, .14)		
Control/ High HardTL	-.05 (.11)	(-.25, .18)	-.04 (.13)	(-.25, .30)
T+N/ Low HardTL	.07 (.12)	(-.18, .30)		
T+N/High HardTL	-.11 (.11)	(-.30, .12)	-.17 (.16)	(-.44, .18)
N/ Low HardTL	.11 (.10)	(-.12, .28)		
N/ High HardTL	.10 (.12)	(-.12, .37)	-.0049 (.14)	(-.22, .36)
N+R/ Low HardTL	.04 (.11)	(-.20, .23)		
N+R/ High HardTL	-.05 (.12)	(-.27, .19)	-.09 (.16)	(-.35, .28)

Note. N = 180

HardTL = Hardware Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

Table I.7. Model 4 – Overall Model Using Social Media Technology Literacy as Moderator and Concern About Information Misuse as Mediator.

	DV1 = CInfoMis	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	1.18 (.86)	-1.09 (.82)
CInfoMis		-.35 (.07)***
Control	-2.06 (1.24)	-.92 (1.18)
T+N	-3.07 (1.40)*	.63 (1.34)
N	-2.96 (1.27)*	-.35 (1.22)
N+R	-.01 (1.24)	1.64 (1.17)
SMedTL	-.26 (.20)	.31 (.19)
Control × SMedTL	.48 (.29)	.15 (.27)
T+N × SMedTL	.73 (.32)*	-.24 (.30)
N × SMedTL	.58 (.29)*	.05 (.28)
N+R × SMedTL	.04 (.29)	-.46 (.27)
R^2	.10*	.20***

Note. N = 177

CInfoMis = Concern about Information Misuse; ContInfo = Contact Information; SMedTL = Social Media Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.8. Model 4 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low SMedTL	.13 (.10)	(-.04, .35)		
Control/ High SMedTL	-.12 (.11)	(-.36, .10)	-.17 (.10)	(-.39, .01)
T+N/ Low SMedTL	.18 (.13)	(-.05, .46)		
T+N/ High SMedTL	-.21 (.12)	(-.45, .02)	-.26 (.13)	**(-.53, -.03)**
N/ Low SMedTL	.33 (.13)	**(.13, .64)**		
N/ High SMedTL	.03 (.11)	(-.20, .25)	-.20 (.11)	**(-.46, -.03)**
N+R/ Low SMedTL	-.04 (.09)	(-.22, .12)		
N+R/ High SMedTL	-.06 (.13)	(-.31, .20)	-.01 (.10)	(-.21, .20)

Note. N = 177

SMedTL = Social Media Technology Literacy; T+N = T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

Table I.9. Model 5 – Overall Model Using Social Media Technology Literacy as Moderator and Companies Should Not Use, Share, and Sell User Information as Mediator.

	DV1 = ComUInfo	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	-1.07 (.80)	-1.53 (.87)
ComUInfo		-.03 (.08)
Control	.45 (1.16)	-.18 (1.25)
T+N	-1.49 (1.30)	1.66 (1.41)
N	-.40 (1.19)	.67 (1.28)
N+R	.59 (1.16)	1.66 (1.25)
SMedTL	.26 (.18)	.41 (.20)*
Control × SMedTL	-.05 (.27)	-.03 (.29)
T+N × SMedTL	.34 (.30)	-.49 (.32)
N × SMedTL	.0029 (.27)	-.15 (.29)
N+R × SMedTL	-.16 (.27)	-.48 (.29)
R^2	.11*	.09

Note. N = 177

ComUInfo = Companies Should Not Use, Share, and Sell User Information; ContInfo = Contact Information; SMedTL = Social Media Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.10. Model 5 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low SMedTL	-.01 (.03)	(-.08, .04)		
Control/ High SMedTL	-.01 (.02)	(-.06, .03)	.00 (.02)	(-.04, .05)
T+N/ Low SMedTL	.01 (.04)	(-.05, .10)		
T+N/ High SMedTL	-.01(.02)	(-.07, .03)	-.01 (.03)	(-.09, .05)
N/ Low SMedTL	.01 (.04)	(-.08, .11)		
N/ High SMedTL	.01 (.04)	(-.07, .10)	-.0001 (.03)	(-.06, .06)
N+R/ Low SMedTL	-.0014 (.03)	(-.07, .04)		
N+R/ High SMedTL	.01 (.03)	(-.05, .07)	.01 (.03)	(-.04, .07)

Note. N = 177

SMedTL = Social Media Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

Table I.11. Model 6 – Overall Model Using Social Media Technology Literacy as Moderator and Concern About Personal Information as Mediator.

	DV1 = CPerInfo	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	-.07 (.85)	-1.53 (.81)
CPerInfo		-.37 (.07)***
Control	.26 (1.22)	-.10 (1.17)
T+N	-1.27 (1.38)	1.24 (1.32)
N	-1.23 (1.26)	.24 (1.20)
N+R	.52 (1.22)	1.83 (1.17)
SMedTL	.02 (.19)	.42 (.18)*
Control × SMedTL	-.04 (.28)	-.04 (.27)
T+N × SMedTL	.31 (.31)	-.38 (.30)
N × SMedTL	.21 (.29)	-.08 (.27)
N+R × SMedTL	-.12 (.29)	-.51 (.27)
R^2	.04	.21***

Note. N = 177

CPerInfo = Concern about Personal Information; ContInfo = Contact Information; SMedTL = Social Media Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.12. Model 6 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low SMedTL	-.04 (.10)	(-.26, .13)		
Control/ High SMedTL	-.01 (.11)	(-.22, .21)	.02 (.09)	(-.15, .23)
T+N/ Low SMedTL	.06 (.12)	(-.19, .28)		
T+N/ High SMedTL	-.11 (.12)	(-.35, .14)	-.11 (.12)	(-.34, .14)
N/ Low SMedTL	.18 (.15)	(-.09, .52)		
N/ High SMedTL	.06 (.13)	(-.20, .31)	-.08 (.13)	(-.36, .16)
N+R/ Low SMedTL	-.04 (.11)	(-.28, .14)		
N+R/ High SMedTL	.02 (.13)	(-.22, .29)	.04 (.11)	(-.14, .29)

Note. N = 177

SMedTL = Social Media Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

Table I.13. Model 7 – Overall Model Using Software Technology Literacy as Moderator and Concern About Information Misuse as Mediator.

	DV1 = CInfoMis	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	.10 (.72)	-.10 (.69)
CInfoMis		-.37 (.07)***
Control	-1.48 (1.12)	-1.87 (1.08)
T+N	-1.91 (1.28)	.19 (1.23)
N	-3.08 (1.27)*	-1.39 (1.24)
N+R	.16 (1.10)	.91 (1.05)
SoftTL	-.02 (.17)	.09 (.16)
Control × SoftTL	.35 (.26)	.36 (.25)
T+N × SoftTL	.48 (.30)	-.14 (.29)
N × SoftTL	.60 (.29)*	.29 (.28)
N+R × SoftTL	.0033 (.27)	-.31 (.26)
R^2	.11*	.20***

Note. N = 180

CInfoMis = Concern about Information Misuse; ContInfo = Contact Information; SoftTL = Software Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.14. Model 7 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low SoftTL	.10 (.12)	(-.13, .35)		
Control/ High SoftTL	-.10 (.12)	(-.33, .13)	-.13 (.12)	(-.37, .08)
T+N/ Low SoftTL	.09 (.13)	(-.15, .35)		
T+N/ High SoftTL	-.18 (.12)	(-.42, .07)	-.18 (.12)	(-.42, .05)
N/ Low SoftTL	.36 (.15)	(.09, .67)		
N/ High SoftTL	.03 (.12)	(-.20, .25)	-.22 (.13)	(-.49, .02)
N+R/ Low SoftTL	-.06 (.10)	(-.26, .12)		
N+R/ High SoftTL	-.07 (.13)	(-.31, .21)	-.0012 (.10)	(-.17, .21)

Note. N = 180

SoftTL = Software Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

Table I.15. Model 8 – Overall Model Using Software Technology Literacy as Moderator and Companies Should Not Use, Share, and Sell User Information as Mediator.

	DV1 = ComUInfo	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	-.29 (.69)	-.14 (.74)
ComUInfo		-.01 (.08)
Control	-.33 (1.08)	-1.32 (1.15)
T+N	-1.63 (1.23)	.88 (1.32)
N	-.46 (1.22)	-.26 (1.31)
N+R	.13 (1.06)	.85 (1.13)
SoftTL	.08 (.16)	.09 (.17)
Control × SoftTL	.12 (.25)	.23 (.27)
T+N × SoftTL	.38 (.29)	-.31 (.31)
N × SoftTL	.01 (.28)	.06 (.30)
N+R × SoftTL	-.06 (.26)	-.31 (.27)
R^2	.08	.07

Note. N = 180

ComUInfo = Companies Should Not Use, Share, and Sell User Information; ContInfo = Contact Information; SoftTL = Software Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.16. Model 8 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low SoftTL	-.0013 (.02)	(-.04, .05)		
Control/ High SoftTL	-.0037 (.03)	(-.07, .05)	-.0016 (.02)	(-.05, .04)
T+N/ Low SoftTL	.0037 (.03)	(-.06, .09)		
T+N/ High SoftTL	-.0036 (.03)	(-.07, .06)	-.0048 (.04)	(-.09, .06)
N/ Low SoftTL	.01 (.04)	(-.09, .10)		
N/ High SoftTL	.01 (.04)	(-.10, .09)	-.0001 (.02)	(-.05, .05)
N+R/ Low SoftTL	.0008 (.02)	(-.04, .04)		
N+R/ High SoftTL	.0019 (.03)	(-.06, .07)	.0007 (.02)	(-.04, .05)

Note. N = 180

SoftTL = Software Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

Table I.17. Model 9 – Overall Model Using Software Technology Literacy as Moderator and Concern About Personal Information as Mediator.

	DV1 = CPerInfo	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	-.10 (.71)	-.17 (.69)
CPerInfo		-.37 (.07)***
Control	.17 (1.10)	-1.26 (1.08)
T+N	-.77 (1.25)	.61 (1.22)
N	-2.88 (1.25)*	-1.32 (1.24)
N+R	.12 (1.08)	.90 (1.06)
SoftTL	.03 (.17)	.11 (.16)
Control × SoftTL	-.03 (.26)	.22 (.25)
T+N × SoftTL	.21 (.29)	-.24 (.29)
N × SoftTL	.59 (.29)*	.28 (.28)
N+R × SoftTL	-.03 (.26)	-.32 (.26)
R^2	.07	.19***

Note. N = 180

CPerInfo = Concern about Personal Information; ContInfo = Contact Information; SoftTL = Software Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.18. Model 9 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low SoftTL	-.03 (.10)	(-.23, .16)		
Control/ High SoftTL	-.02 (.11)	(-.23, .22)	.01 (.10)	(-.17, .21)
T+N/ Low SoftTL	.02 (.12)	(-.23, .23)		
T+N/ High SoftTL	-.10 (.13)	(-.34, .17)	-.08 (.12)	(-.29, .18)
N/ Low SoftTL	.30 (.15)	**(.01, .60)**		
N/ High SoftTL	-.03 (.13)	(-.27, .23)	-.22 (.13)	(-.47, .05)
N+R/ Low SoftTL	-.01 (.10)	(-.23, .16)		
N+R/ High SoftTL	.01 (.14)	(-.25, .30)	.01 (.11)	(-.17, .27)

Note. N = 180

SoftTL = Software Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

Table I.19. Model 10 – Overall Model Using Comparative Knowledge Technology Literacy as Moderator and Concern About Information Misuse as Mediator.

	DV1 = CInfoMis	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	1.26 (1.05)	-.91 (.96)
CInfoMis		-.34 (.07)***
Control	-1.42 (1.41)	-1.33 (1.28)
T+N	-1.79 (1.30)	.48 (1.19)
N	-2.41 (1.50)	-.51 (1.37)
N+R	-1.20 (1.32)	1.23 (1.20)
CKnowTL	-.29 (.25)	.28 (.23)
Control × CKnowTL	.35 (.34)	.27 (.31)
T+N × CKnowTL	.46 (.31)	-.21 (.28)
N × CKnowTL	.47 (.35)	.10 (.32)
N+R × CKnowTL	.33 (.32)	-.39 (.29)
R^2	.07	.21***

Note. N = 179

CInfoMis = Concern about Information Misuse; ContInfo = Contact Information; CKnowTL = Comparative Knowledge Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.20. Model 10 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low CKnowTL	.08 (.09)	(-.09, .25)		
Control/ High CKnowTL	-.10 (.12)	(-.34, .14)	-.12 (.09)	(-.30, .07)
T+N/ Low CKnowTL	.07 (.10)	(-.12, .30)		
T+N/ High CKnowTL	-.17 (.11)	(-.40, .05)	-.15 (.09)	(-.36, .01)
N/ Low CKnowTL	.26 (.10)	**(.06, .46)**		
N/ High CKnowTL	.02 (.14)	(-.25, .30)	-.16 (.11)	(-.37, .07)
N+R/ Low CKnowTL	.02 (.08)	(-.13, .18)		
N+R/ High CKnowTL	-.16 (.12)	(-.42, 07)	-.11 (.09)	(-.31, .04)

Note. N = 179

CKnowTL = Comparative Knowledge Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

Table I.21. Model 11 – Overall Model Using Comparative Knowledge Technology Literacy as Moderator and Companies Should Not Use, Share, and Sell User Information as Mediator.

	DV1 = ComUInfo	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	-.47 (.98)	-1.34 (1.02)
ComUInfo		-.02 (.08)
Control	.14 (1.32)	-.85 (1.36)
T+N	-.43 (1.21)	1.07 (1.26)
N	.84 (1.40)	.31 (1.45)
N+R	1.22 (1.23)	1.65 (1.28)
CKnowTL	.13 (.23)	.38 (.24)
Control × CKnowTL	.02 (.32)	.15 (.33)
T+N × CKnowTL	.10 (.29)	-.37 (.30)
N × CKnowTL	-.30 (.33)	-.07 (.34)
N+R × CKnowTL	-.33 (.30)	-.50 (.31)
R^2	.07	.10*

Note. N = 179

ComUInfo = Companies Should Not Use, Share, and Sell User Information; ContInfo = Contact Information; CKnowTL = Comparative Knowledge Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.22. Model 11 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low CKnowTL	-.0035 (.03)	(-.06, .05)		
Control/ High CKnowTL	-.0040 (.03)	(-.08, .06)	-.0003 (.02)	(-.06, .05)
T+N/ Low CKnowTL	.0012 (.02)	(-.05, .06)		
T+N/ High CKnowTL	-.0016 (.03)	(-.06, .05)	-.0018 (.03)	(-.06, .05)
N/ Low CKnowTL	.0033 (.03)	(-.07, .06)		
N/ High CKnowTL	.01 (.06)	(-.12, .15)	.01 (.04)	(-.07, .10)
N+R/ Low CKnowTL	-.0011 (.02)	(-.05, .04)		
N+R/ High CKnowTL	.01 (.05)	(-.09, .11)	.01 (.04)	(-.06, .09)

Note. N = 179

CKnowTL = Comparative Knowledge Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

Table I.23. Model 12 – Overall Model Using Comparative Knowledge Technology Literacy as Moderator and Concern About Personal Information as Mediator.

	DV1 = CPerInfo	DV2 = ContInfo
	b (*SE*)	*b* (*SE*)
Constant	1.01 (1.02)	-.97 (.95)
CPerInfo		-.36 (.07)***
Control	-1.09 (1.36)	-1.24 (1.28)
T+N	-1.22 (1.26)	.64 (1.18)
N	-2.35 (1.45)	-.54 (1.36)
N+R	-.26 (1.28)	1.54 (1.19)
CKnowTL	-.23 (.24)	.30 (.23)
Control × CKnowTL	.28 (.33)	.25 (.31)
T+N × CKnowTL	.32 (.30)	-.25 (.28)
N × CKnowTL	.49 (.34)	.11 (.32)
N+R × CKnowTL	.05 (.31)	-.48 (.29)
R^2	.04	.22***

Note. N = 179

CPerInfo = Concern about Personal Information; ContInfo = Contact Information; CKnowTL = Comparative Knowledge Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples.

**p* < .05. ***p* < .01. ****p* < .001

Table I.24. Model 12 – Conditional Indirect Effects.

			Index	
	b (*SE*)	95% CI	*b* (*SE*)	95% CI
Control/ Low CKnowTL	.05 (.09)	(-.12, .22)		
Control/ High CKnowTL	-.11 (.13)	(-.36, .15)	-.10 (.10)	(-.31, .10)
T+N/ Low CKnowTL	.04 (.10)	(-.14, .25)		
T+N/ High CKnowTL	-.14 (.13)	(-.39, .12)	-.11 (.10)	(-.33, .09)
N/ Low CKnowTL	.23 (.13)	(-.03, .49)		
N/ High CKnowTL	-.04 (.15)	(-.33, .28)	-.18 (.14)	(-.43, .12)
N+R/ Low CKnowTL	.03 (.09)	(-.14, .21)		
N+R/ High CKnowTL	.0047 (.14)	(-.27, .28)	-.02 (.10)	(-.21, .18)

Note. N = 179

CKnowTL = Comparative Knowledge Technology Literacy; T+N = Traditional Content + Neutral Examples; N = Neutral Examples; N+R = Neutral Examples + Risk Examples; Index = Index of Moderated Mediation.

BIBLIOGRAPHY

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). *Privacy in E-commerce: Examining user scenarios and privacy preferences*. ACM Conference on Electronic Commerce, 1-8.

Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy*, 26-33.

Berscheid, E. (1977). Privacy: A hidden variable in social psychology. *Journal of Social Issues*, *33*, 85–101.

Chellappa, R. K., & Sin, R. (2005). Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, *6*, 181-202.

Ding, D., Cooper, R.A., Pasquina, P.F., & Fici-Pasquina, L. (2011). Sensor technology for smart homes. *Maturitas, 69*, 131-136. doi: 10.1016/j.maturitas.2011.03.016

Fazio, R.H., Zanna, M.P., & Cooper, J. (1978). Direct experience and attitude-behavior consistency: An information process analysis. *Personality and Social Psychology Bulletin*, *4*(1), 48-51. doi:10.1177/014616727800400109

Fitbit Privacy Policy. (n.d.). Retrieved October 11, 2017, from https://www.fitbit.com/legal/privacy-policy

GE Connected Data Privacy Policy. (n.d.). Retrieved October 11, 2017, from http://www.geappliances.com/privacy/privacy_policy_connected.htm

GE WiFi Connect. (n.d.). Retrieved October 11, 2017, from http://www.geappliances.com/ge/connected-appliances/

Gigerenzer, G., & Goldstein, D. G. (1996). Reasoning the fast and frugal way: Models of bounded rationality. *Psychological Review, 103*(4), 650-669.

Hayes, A.F. (2018). Conditional Process Analysis with a Multicategorical Antecedent. In D.A. Kenny & T.D. Little (Eds.), *Introduction to Mediation, Moderation, and Conditional Process Analysis, Second Edition: A Regression-Based Approach* (pp. 469-503). New York, NY: Guilford Publications.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, *42*(4), 80–85.

Jensen, C., & Potts, C. (2004). *Privacy policies on decision-making tools: An evaluation of online privacy notices.* CHI. Vienna, Austria. 471-478.

LG SmartThinQ. (n.d.). Retrieved October 11, 2017, from http://www.lg.com/us/discover/smartthinq/thinq

McDonald, A. M., & Cranor, L. F. (2009). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for Information Society*, *4*(3), 543-568.

Metzger, M. (2004). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*, *9*(4), 00. doi: 10.1111/j.1083-6101.2004.tb00292.x

Metzger, M. J., & Docter, S. (2003). Public opinion and policy initiatives for online privacy protection. *Journal of Broadcasting & Electronic Media*, *47*(3).

Montano, C.F., Lundmark, M., & Mahr, W. (2006). Control vs convenience: Critical factors of smart homes. 2nd Scandinavian Student Interaction Design Research Conference.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research*, *40*, 215–236. doi:10.1177/0093650211418338

Parker, P., & Tavassoli, N. T. (1997). *Physioeconomic Theories of Culture and Consumption*. Fontainebleau, France: INSEAD.

Ponte, E. R., Carvajal-Trujillo, E., & Escobar-Rodríguez, T. (2015). Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents. *Tourism Management*, *47*, 286-302.

Ray, S., Ow, T., & Kim, S. S. (2011). Security assurance: how online service providers can influence security control perceptions and gain trust. *Decision Sciences, 42*(2), 391–412, doi:10.1111/j.1540-5915.2011.00316.x

Samsung CHEF collection. (n.d.). Retrieved October 11, 2017, from https://www.samsung.com/us/explore/chef-collection/

Samsung Privacy Policy—SmartTV Supplement. (n.d.) Retrieved October 11, 2017, from http://www.samsung.com/sg/info/privacy/smarttv/

Selten, R., (1999). *What is bounded rationality? Paper prepared for the Dahlem Conference 1999*. Sonderforschungsbereich (SFB) 303 Discussion Paper No. B-454.

Simon, H. A. (1957). *Models of Man, Social and Rational: Mathematical Essays on Rational Human Behavior in a Social Setting*. New York: John Wiley and Sons.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001, 14-17 October). *E-Privacy in second generation E-commerce: Privacy preferences versus actual behavior*. Proceedings of the 3rd ACM Conference on Electronic Commerce, 38–47.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36–49.

The Center for the Digital Future at USC Annenberg (2015). *Surveying the Digital Future*. Retrieved from http://www.digitalcenter.org/wp-content/uploads/2013/06/2015-Digital-Future-Report.pdf

The Center for the Digital Future at USC Annenberg (2017). *Surveying the Digital Future*. Retrieved from http://www.digitalcenter.org/wp-content/uploads/2018/04/2017-Digital-Future-Report-2.pdf

Tsai, K. P., Chien, S. F., & Cheng, H. M. (2003). Towards a machine for living: A literature survey of smart homes. *Digital Designs: 21st eCAADe Conference Proceedings,* 419-422. eCAADe: Conferences. Graz, Austria.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254-268. Doi: 10.1287/isre.1090.0260

Turow, J., Feldman, L., & Meltzer, K. (2005). *Open to exploitation: American shoppers online and offline.* A Report from the Annenberg Public Policy Center of the University of Pennsylvania.

Twitter Privacy Policy. (n.d.) Retrieved October 11, 2017, from https://twitter.com/en/privacy

VIZIO Privacy Policy. (n.d.) Retrieved October 11, 2017, from https://www.vizio.com/privacy

Xu, H., & Teo, H. H. (2004). *Alleviating Consumer's Privacy Concern in Location-Based Services: A Psychological Control Perspective.* Proceedings of the Twenty-Fifth Annual International Conference on Information Systems. Washington, D. C., United States. 793-806.

VITA

Delicia Anceisao Vaz was born in Bombay, India. She earned her Bachelor of Arts degree in Chemistry and Bachelor of Arts degree in Biology from the University of Missouri – Kansas City in May 2013. She earned her Master of Science degree in Industrial-Organizational Psychology from the Missouri University of Science and Technology in July 2018. During the course of her graduate curriculum, she was involved in Dr. Denise A. Baker's research project related to the National Science Foundation/ National Institute of Food and Agriculture, smart living, cyber physical human systems, and social behavioral models.