Help Wanted: Consumer Privacy Behavior and Smart Home Internet of Things (IoT) Devices

Marc Dupuis
Computing and Software Systems
University of Washington Bothell
Bothell Washington U.S.A.
marcjd@uw.edu

Mercy Ebenezer
Computing and Software Systems
University of Washington Bothell
Bothell Washington U.S.A.
mercyebe@uw.edu

ABSTRACT

The infrastructure of smart home IoT devices is complex and the combination of data streams that run throughout it is convoluted. This poses a threat to consumer privacy. However, consumers fall short of adopting privacy protection measures. This study employed two qualitative and one quantitative research methodology in a mixed method research design to examine the role of privacy preferences with respect to home IoT devices. Protection Motivation Theory was used as the theoretical framework. Results suggest that individuals do care about the dangers associated with having one's privacy violated by an IoT device and are more willing to engage in protective measures if they believe they are able to understand the various mechanisms for doing so, but only if the costs are not too high. However, consumers in general have little knowledge related to the privacy issues rampant in smart home IoT devices, but do appear concerned when presented with that information directly.

CCS CONCEPTS

Security and privacy → Human and societal aspects of security and privacy • Security and privacy → Security in hardware → Embedded systems security

KEYWORDS

Consumer IoT devices; privacy; security; Protection Motivation Theory; mixed methods; interviews; survey; content analysis.

ACM Reference format:

M. Dupuis and M. Ebenezer. 2018. Help Wanted: Consumer Privacy Behavior and Smart Home Internet of Things (IoT) Devices. In *Proceedings of ACM SIGITE conference (SIGITE '18). Fort Lauderdale, FL, USA October 3–6, 2018*, 6 pages. https://doi.org/10.1145/3241815.3241869

SIGITE '18, October 3–6, 2018, Fort Lauderdale, FL, USA

ACM ISBN 978-1-4503-5954-2/18/10…$15.00
https://doi.org/10.1145/1234567890

1 Introduction

IoT has a wide range of application areas: transportation and logistics, healthcare, smart environment (home, office, plant), and personal and social domains [1]. These domain areas connect different parts of the community and enable each entity within that community to work efficiently [2]. This large-scale expansion and integration is associated with an increase on the business front as well. According to Business Insider, $6 trillion will be spent on IoT solutions in the next 10 years and 34 billion devices will be connected to the Internet by 2020, more than triple the 10 billion connected devices in 2015 [3].

Besides the application areas mentioned above, the need for smart home automation systems is increasing at a good pace [4]. It is estimated that smart home IoT devices will exhibit the highest increase in the next five years when compared to other subcategories of smart city devices, such as health care, public services, smart commercial buildings, transport, and utilities [5]. This finding from Gartner and The Deloitte Consumer Review highlights the importance of considering smart home IoT devices and the surrounding privacy issues and concerns.

The infrastructure of smart home IoT devices is complex and the combination of data streams that run throughout it is convoluted. Additionally, the creative interconnection of everyday objects and devices within the infrastructure can be dangerous because of the large amount of sensitive data collected, shared, and stored. This poses a threat to consumer privacy [6]. One of the manifestations of the identity privacy issue is constant monitoring of consumers without their knowledge. This type of invasion into a consumer's personal space often leads to privacy violations and raises definitive privacy concerns [6], [7].

The solution providers of smart home IoT devices must begin to consider privacy issues with greater seriousness to best serve consumers' interests and needs [8]. However, IoT solution providers' responses to these initiatives are less pronounced when compared to their rampant efforts to expand their business or to exhibit significant progress in the technological front [3]. When IoT solution providers exhibit little or no interest in fulfilling privacy requirements, the responsibility shifts to consumers.

However, consumers fall short of adopting privacy protection measures. Therefore, this study explores privacy behavior as it relates to the privacy protection measures consumers engage in with respect to smart home IoT devices and their overall understanding of the risks.

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

Privacy policy statements for home IoT devices often appear on the official IoT device's website rather than the product package [9]. This is often inconvenient for consumers and does not account for best practices in privacy protection. The statements also are long and contain complicated language that makes them difficult for the user to comprehend and consequently exhibit protective behavior. In addition, home IoT devices have small displays and no clear indication of the input and output areas; this restricts the consumers from reading the policy statements on the device itself [9].

For these reasons, this study focuses on understanding the implications of the abovementioned limitations on consumer privacy behavior as it relates to smart home IoT devices. We do this by examining customer reviews of home IoT devices and then conducting interviews on the consumers' understanding and the perceptions they have as it relates to privacy on these types of devices. Finally, we conduct a large-scale survey using Protection Motivation Theory (PMT) as the theoretical framework in which to understand the privacy dynamic of individuals in the IoT space.

2 Literature Review

This study characterizes consumer privacy behavior by establishing privacy preferences and adopting privacy education. Privacy preferences allow consumers to be informed on the methods of data collection, storing, and sharing employed by devices in general. This knowledge encourages consumers to disclose personal and sensitive data based on their preferences. Privacy education through online articles, blogs, and forums inform the consumer on the existing privacy issues in devices and applications.

Additionally, adopting privacy behavior in an online environment requires a certain amount of skill and technical knowledge. For instance, in one particular study adults were able to adopt protective behavior in the online environment because they were more efficient in gathering privacy related information when compared to young adolescents [10]. In another study that investigated users' reaction to disclosure of personal information on mobile applications, security-aware users were more careful and reluctant in giving away personal information when compared to security unaware users [11].

IoT systems have multiple users and each user has different privacy preferences [12], which may also vary based on one's personality or affect [13], [14]. For instance, a home monitoring IoT device will collect video data of all members of the household, including guests who visit. In such a case, it is hard to establish privacy preferences with respect to a single person for a home IoT device. Most home IoT devices have small displays with no clear input and output areas; this makes it difficult for the user to read privacy policies on the device [9]. This means the consumer must read these policies from the official IoT device's website or the manufacturer's website [9].

From the above discussion, we argue that a clear lack of easy access to adopt privacy protection measures exists. This prevents consumers from adopting privacy behavior. Several factors are at play. The privacy behavior towards home IoT devices are affected by factors such as time, effort, cognitive manipulation of web experience, lack of privacy information during the purchase decision process, and lack of technical skill.

2.1 Protection Motivation Theory

Protection Motivation Theory (PMT) serves as the primary theoretical framework used to help guide this research. In particular, PMT has been used extensively in both health behavior research [15] and cyber security and privacy research [22] to help better understand what motivates individuals to engage in protective behaviors.

Developed in 1975, PMT is an extension of expectancy-value theory with an aim to provide a more complete understanding of the effects of fear appeals on attitude change [18]. A fear appeal is a communication of a threat to a person that provides information related to one's well-being [19, p. 107]. It is used "in persuasive messages to scare people in the hopes that the aroused fear will result in the performance of adaptive behaviors" [20, p. 49]. When a fear appeal is presented to an individual, two independent processes occur: threat appraisal and coping appraisal.

Threat appraisal consists of perceived threat severity (i.e., the potential impact of the threat) and perceived threat vulnerability (i.e., the likelihood of the threat impacting them) [18]. Coping appraisal consists of self-efficacy (i.e., one's belief in being able to engage in protective behaviors), perceived response efficacy (i.e., one's belief that a given protective response will be effective in mitigating the threat), and perceived response costs (i.e., one's estimation of how much time, energy, and effort will be require to engage in a protective behavior) [18]. The greater the perceived threat severity and perceived threat vulnerability then the greater likelihood an individual will engage in a protective behavior as the threat is seen as more significant. Likewise, the greater their belief in being able to carry out a protective behavior (i.e., self-efficacy) and that this behavior will be effective (i.e., perceived response efficacy), then the greater likelihood they will initiate this behavior. However, if the cost of doing so (i.e., perceived response costs) is too great, then the less likely it will be for an individual to engage in such protective behavior.

Since this study consists of both qualitative and quantitative methodologies, PMT will be used to help inform lines of inquiry during the qualitative data collection process. Likewise, constructs from PMT will be measured during the quantitative data collection phase. For the quantitative data, we present the following hypotheses:

H1: Greater levels of perceived threat severity related to having one's privacy compromised due to an IoT device will

result in higher levels of performing behavior to mitigate this threat.

H2: Greater levels of perceived threat vulnerability related to having one's privacy compromised due to an IoT device will result in higher levels of performing behavior to mitigate this threat.

H3: Greater levels of self-efficacy related to the responses necessary to prevent one's privacy from being compromised due to an IoT device will result in higher levels of performing behavior to mitigate this threat.

H4: Greater levels of perceived response efficacy related to the responses necessary to prevent one's privacy from being compromised due to an IoT device will result in higher levels of performing behavior to mitigate this threat.

H5: Lower levels of perceived response costs related to the responses necessary to prevent one's privacy from being compromised due to an IoT device will result in higher levels of performing behavior to mitigate this threat.

Next, the methods that were employed will be discussed.

3 Methods

In this study, a mixed methods research design was employed consisting of three methods to explore the dynamics of individuals as it relates to the privacy of home IoT devices [21], [22]. First, we examined customer reviews by selecting 50 reviews for each of the top 10 home IoT devices. Our goal here was to examine the extent privacy issues would come up in reviews left by customers. Second, we interviewed 18 participants to gauge their understanding of and concern with privacy as it relates to IoT devices. Finally, we conducted a large-scale survey to examine the constructs of PMT in the context of these devices.

3.1 Customer Reviews

Five hundred customer reviews of the top 10 smart home IoT devices were collected from the Amazon.com website. The selection criteria for these top 10 devices was based on Gartner's listing of smart home sub-categories [5] and Amazon's best sellers in the smart home category. The selection for the top 10 devices was performed on Amazon's best sellers in the smart home category on February 14th, 2017. Multiple iterations were followed to finalize the selection list because best seller tags on the devices tend to change according to sales at a given point in time.

The customer reviews of verified purchases were grouped based on two categories: rating scale and review groups. The rating scale ranged from 1 to 5 and the review groups consisted of top reviews and recent reviews. The 500 reviews were equally divided among the 10 devices based on the abovementioned categories. In order to obtain a diverse cross-section of reviews by consumers, we collected an equal number of reviews for each rating (i.e., 1-5) for each of the two categories previously mentioned (i.e., top reviews and recent reviews). In total, fifty reviews for each of the 10 devices were collected. This grouping and distribution was replicated for the remaining nine home IoT devices.

After the data was collected, appropriate qualitative data analysis procedures were used to code the large number of reviews [23]. The coding strategies generated six major themes. These themes were later applied throughout the data to produce subthemes. Some necessary subthemes were introduced and removed accordingly to reconcile the differences within the large data set. After the coding process, the themes were explained and useful insights were recorded. Two coders working independently from one another coded the reviews. Insights from the themes identified here would help inform the development of questions for the semi-structured interviews that would follow.

3.2 Interview Data

Interview sessions were conducted among 18 student participants from a public university. Participants were selected to maximize a gender balance and diversity of educational backgrounds (i.e., majors). The participants were questioned on the following aspects: privacy behavior, knowledge of privacy issues in home IoT devices, impact of privacy behavior on the purchase decision process, among other subtopics. The constructs from PMT were also used to help frame some of the questions used during this process. The interview data was later transcribed and coded using appropriate coding strategies suggested by Brown et al. [24]. Two coders were using during this process with a subset of the transcripts coded by both. If discrepancies were found in the themes being uncovered, a joint session was held to clarify such discrepancies and any previously coded transcripts were recoded with this insight and consensus in mind. The insights from the coding process were noted.

Because there was a discrepancy in understanding the definition of smart home IoT devices and privacy issues in these devices, articles were handed out to the participants to address this discrepancy. These articles were sections from a published report, "A HP study on IoT security", released by the Hewlett Packard company. They informed participants on existing privacy issues in home security IoT devices and other security related issues. This helped the participants to convey their thoughts and impressions, and establish their baseline knowledge on data collection methods in IoT systems, among other privacy issues.

3.3 Survey Data

To collect survey data, we used Amazon's Mechanical Turk, which has been shown to be a generally reliable and efficient method of collecting data for surveys while also providing a generally high level of anonymity for participants [25], [26]. We adapted items from various sources to measure the constructs associated with PMT: perceived threat severity [27], perceived threat vulnerability [27], self-efficacy [28], perceived response costs [29], and perceived response efficacy [27].

However, in order to simplify the measures related to the coping constructs, we opted to identify a general response to the threat of having one's personal information or privacy compromised due to IoT devices. In particular, we assessed one's

ability to understand the privacy risks of IoT devices so that the threat could be mitigated rather than a series of specific actions. This was done due to the exploratory nature of this study and the general lack of understanding that persists from consumers with respect to IoT devices. Thus, we did not measure specific tasks, but the measures are within the same domain [30], [31].

Finally, we used recommendations from the literature cited earlier and a review by subject matter experts to identify some behaviors necessary to mitigate the threat of having one's privacy violated or personal information compromised due to an IoT device. These formative indicators and the associated reflective indicators for the constructs associated with PMT may be found in the Appendix.

The data collected was analyzed using IBM SPSS version 19 and SmartPLS v. 3.2.4 [32]. This included an assessment of both the measurement model and structural model.

4 Results

4.1 Qualitative Analysis of Customer Reviews

The customer reviews collected from the Amazon.com website provided insights into the amount of concern consumers expressed in smart home IoT devices as it relates to privacy. The website served as an effective platform to understand consumer privacy behavior from the customer reviews and comments.

The information in the reviews indicated several factors that influence a consumer's purchase decision. The major themes that emerged from coding the customer reviews were need, cost, features, ease of use, usefulness, convenience, comfort, privacy, security, and integration with other devices. The primary concern of most consumers revolved around constructs from the Technology Acceptance Model, such as ease of use and usefulness of smart home IoT devices [33], [34].

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

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

Five out of the six reviews were categorized as "top reviews" by the website. Top reviews are those voted as most helpful reviews by other consumers interested in the same device as the writer of the top review. This is a possible indication that consumers considered those reviews important and helpful to some degree and did not ignore them completely. In other words, if consumers ignored these reviews, they could not have appeared in the "top review" category.

However, the five top reviews also included issues relating to cost, features, functionality, integration to other devices, among other issues. This means there could have been some other information that was of interest to the reader that prompted her to vote the review as 'helpful'. Additionally, some of the reviews that contained detailed concerns over privacy issues suggested that the writers may have prior technical knowledge that helped them write the review. Most of these privacy issues related to video data collected by home monitoring systems with IP traceable web cams.

4.2 Qualitative Analysis of Interview Data

Insights gained from the results from the first method just described were incorporated into our interviews with the 18 participants. In particular, we were curious how these participants evaluated smart home IoT devices from a privacy perspective during the purchase decision process, if at all. Likewise, based on the customer reviews we wanted to determine how salient of an issue privacy was for our participants.

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

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

Adopting privacy protection measures for smart home IoT devices is not as common as the cost–benefit analysis method that consumers adopt during their purchase decision process. The cost–benefit analysis method was used to compare entities such as price, features, and functionality of a device. Among privacy protection measures, adopting privacy education was fairly easy to perform when compared to establishing privacy preferences. However, during the study when information on privacy issues was easily made available through hand distribution of articles, most participants exhibited a strong inclination towards discussing the issues. This inclination has a large impact in the way consumers make their purchase decisions.

In the real world, however, there will not be someone there to provide them with an easy to read handout as we did in this study. This further illustrates the disconnect between the interest consumers supposedly have in privacy issues and the actual behavior exhibited when it comes time to make decisions with the potential to adversely impact their privacy.

The lack of baseline knowledge and forethought discovered here as it related to smart home IoT devices led us to be cautious in the level of granularity employed in the large-scale survey that would follow. In particular, self-efficacy is generally a measure that should be assessed at the task level. In other words, general questions should normally be avoided. However, based on the results obtained here and the lack of overall attention related to privacy as detailed in the analysis of customer reviews, we opted to measure self-efficacy at a more general level. Our interest was in knowing whether or not one's belief in being able to protect themselves from privacy issues as it related to IoT devices would result in them engaging in such protective behaviors. It did not make sense given what we learned from these first two stages of our study to ask them questions related to tasks for which they would be completely unfamiliar.

4.3 Quantitative Analysis of Survey Data

In this section, we discuss the results of the survey. Overall, 1,006 valid responses were received after invalid responses were removed, which included approximately 11% of participants failing a quality control question. Common method bias, reliability, validity, and the structural model are discussed next.

4.3.1 Common Methods Bias. Multiple methods were employed in this study, but within an analysis of a single method, such as survey data collection, the risk of bias due to the method itself must be considered. There are techniques available to help address common method bias and they were employed in the current study [35]. For example, a high level of anonymity is provided by using Amazon's Mechanical Turk.

Thus, steps were taken to mitigate the threat of common method bias. Regardless, it remains a concern. Therefore, we performed post hoc analysis of the data, including Harman's single factor test with both confirmatory factor analysis and exploratory factor analysis [35], [36]. The total variance explained by a single factor was below the threshold of 50%, which supports the notion that common method bias was not a significant factor.

4.3.2 Reliability. We began by assessing the reliability of the constructs. The focus of this analysis began in SPSS and was concerned with the reflective indicators, which all of the independent variables were comprised of. Once this was complete, we examined reliability in our measurement model. Indicators with loadings less than 0.65 were removed. This was not a concern with respect to content validity since the indicators in question were all reflective. Cronbach's Alpha was above 0.80 in each case.

4.3.3 Validity. Beyond an analysis of reliability, it is important to also assess validity. We did this by using the AVE calculated in SmartPLS version 3.2.4 [32]. The composite reliability values were greater than the AVE. Additionally, the AVE was greater than the minimum 0.500 threshold [37]. Thus, convergent validity was found in the current study. Information on the correlations between latent constructs may be found at: http://faculty.washington.edu/marcjd/supplemental/sigite2018/

We also conducted an analysis to assess discriminant validity. The indicators and blocks of indicators loaded higher with the construct they were intended to measure rather than another construct. Furthermore, we employed the Heterotrait-Monotrait Ratio (HTMT) technique to verify that discriminant validity was met [38]. Discriminant validity was indicated in all cases.

4.3.4 Structural Model. The structural model supported three out of five hypotheses. The variance explained by the model was 20.4% (adjusted R^2). Figure 1 illustrates these results.

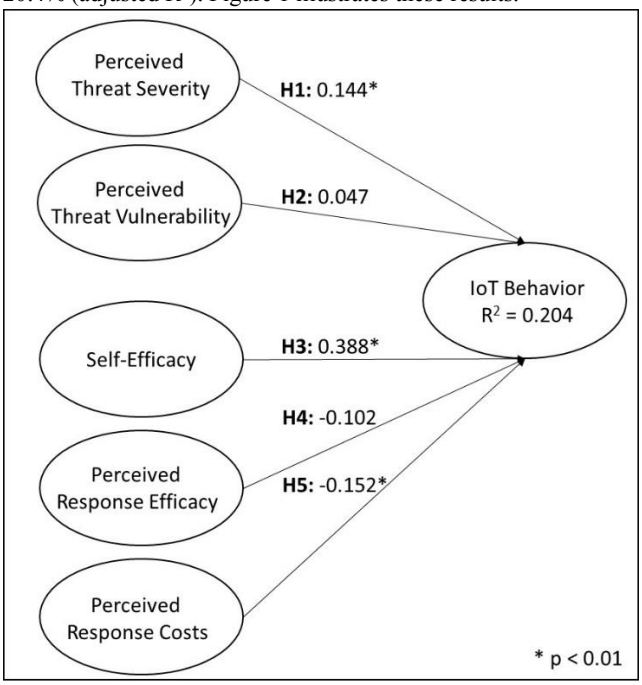

Figure 1: Structural Model

The effectiveness of a mitigating response did not receive sufficient support based on the responses received by participants, nor did the perceived threat vulnerability of individuals. Overall, PMT appears to be an effective theoretical framework to understand the dynamics of privacy concerns with home IoT devices. A contribution made from a theoretical standpoint is how PMT may be used to understand privacy concerns with smart home IoT devices—even when information on specific tasks required is lacking due to lower levels of baseline knowledge.

5 Discussion

This study contributes to the body of knowledge in understanding the impact of consumer behavior and concern with respect to the privacy of smart home IoT devices. The purchase decision process and subsequent evaluation of purchases smart home IoT devices is a good place to begin with as it provides in-depth understanding

into a consumer's concern in this arena. This study helps inform us on the factors that affect a consumer's purchase choice and the influence of perceived threat severity, perceived threat vulnerability, self-efficacy, perceived response efficacy, and perceived response costs on the consumers' privacy behavior. This study also helps inform us on the lack of easy access to privacy protection measures being the primary cause for privacy trade-offs with convenient purchase choices.

A limitation of this study includes the possibility that participants could have made statements consistent with either what they thought the interviewer wanted to hear or the researcher in the case of the survey. While several methodologies are susceptible to satisficing, it is something that must nonetheless be considered. Regardless, significant insight was gained despite this limitation.

Overall, this study employed two qualitative and one quantitative research methodology to examine the role of privacy preferences with respect to home IoT devices. PMT was used as the theoretical framework in which to view this issue. This not only helped inform lines of inquiry during the interviews, but it also provided testable hypotheses for the survey data that was collected. Three out of five hypotheses were supported. This suggests that individuals do care about the dangers associated with having one's privacy violated by an IoT device and are more willing to engage in protective measures if they believe they are able to understand the various mechanisms for doing so, but only if the costs are not too high.Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here. Insert paragraph text here.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[3] J. Camhi and J. Greenough, "Here are IoT trends that will change the way businesses, governments, and consumers interact with the world," *Business Insider*, 29-Aug-2016. [Online]. Available: http://www.businessinsider.com/top-internet-of-things-trends-2016-1. [Accessed: 27-May-2017].

[4] The Deloitte Consumer Review, "Switch on to the connected home." Jul-2016.

[5] "Gartner Says Smart Cities Will Use 1.6 Billion Connected Things in 2016," 07-Dec-2015. [Online]. Available: http://www.gartner.com/newsroom/id/3175418. [Accessed: 15-Feb-2017].

[6] L. In, *The Internet of Things in the Modern Business Environment*. IGI Global, 2017.

[7] M. Dupuis, R. Crossler, and B. Endicott-Popovsky, "Measuring the Human Factor in Information Security and Privacy," in *The 49th Hawaii International Conference on System Sciences (HICSS)*, Kauai, Hawaii, 2016.

[8] M. K. Ohlhausen, "Privacy Challenges and Opportunities: The Role of the Federal Trade Commission," *J. Public Policy Mark.*, vol. 33, no. 1, pp. 4–9, Spring 2014.

[9] S. R. Peppet, "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent," *Tex. Law Rev.*, vol. 93, p. 85, 2014.

[10] S. Youn, "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents," *J. Consum. Aff.*, vol. 43, no. 3, pp. 389–418, Sep. 2009.

[11] N. Eling *et al.*, "Investigating Users' Reaction to Fine-Grained Data Requests: A Market Experiment," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Los Alamitos, CA, USA, 2016, pp. 3666–3675.

[12] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 1–17.

[13] M. Dupuis, S. Khadeer, and J. Huang, "'I Got the Job!': An Exploratory Study Examining the Psychological Factors Related to Status Updates on Facebook," *Comput. Hum. Behav.*, vol. 73, pp. 132–140, 2017.

[14] M. Dupuis, "'Wait, Do I Know You?': A Look at Personality and Preventing One's Personal Information from being Compromised," in *Proceedings of the 5th Annual Conference on Research in Information Technology*, Boston, MA, USA, 2016, pp. 55–55.

[15] D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers, "A Meta-Analysis of Research on Protection Motivation Theory," *J. Appl. Soc. Psychol.*, vol. 30, no. 2, p. 407, 2000.

[16] R. Crossler, "Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data," in *The 43rd Hawaii International Conference on System Sciences (HICSS)*, Koloa, Kauai, Hawaii, 2010, p. 10.

[17] M. Dupuis, R. Crossler, and B. Endicott-Popovsky, "The Information Security Behavior of Home Users: Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information," presented at the The Dewald Roode Information Security Workshop, Provo, Utah, 2012.

[18] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *J. Psychol.*, vol. 91, no. 1, p. 93, 1975.

[19] S. Milne, P. Sheeran, and S. Orbell, "Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory.," *J. Appl. Soc. Psychol.*, vol. 30, no. 1, 2000.

[20] D. R. Roskos-Ewoldsen and H. J. R. Yu, "Fear appeal messages affect accessibility of attitudes toward the threat and adaptive behaviors," *GCMM Commun. Monogr.*, vol. 71, no. 1, pp. 49–69, 2004.

[21] V. Venkatesh, S. A. Brown, and H. Bala, "Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems.," *MIS Q.*, vol. 37, no. 1, 2013.

[22] V. Venkatesh, S. A. Brown, and Y. W. Sullivan, "Guidelines for conducting mixed-methods research: An extension and illustration," *J. Assoc. Inf. Syst.*, vol. 17, no. 7, p. 435, 2016.

[23] M. F. Chowdhury, "Coding, sorting and sifting of qualitative data analysis: debates and discussion," *Qual. Quant.*, vol. 49, no. 3, pp. 1135–1143, 2015.

[24] J. Brown, J. H. Sorrell, J. McClaren, and J. W. Creswell, "Waiting for a Liver Transplant," *Qual. Health Res.*, vol. 16, no. 1, pp. 119–136, Jan. 2006.

[25] M. Dupuis, B. Endicott-Popovsky, and R. Crossler, "An Analysis of the Use of Amazon's Mechanical Turk for Survey Research in the Cloud," presented at the International Conference on Cloud Security Management, Seattle, Washington, 2013.

[26] Z. R. Steelman, B. I. Hammer, and M. Limayem, "Data Collection in the Digital Age: Innovative Alterantives to Student Samples.," *MIS Q.*, vol. 38, no. 2, pp. 355–378, 2014.

[27] K. Witte, K. A. Cameron, J. K. McKeon, and J. M. Berkowitz, "Predicting risk behaviors: Development and validation of a diagnostic scale.," *J. Health Commun.*, vol. 1, no. 4, pp. 317–341, 1996.

[28] B.-Y. Ng and M. A. Rahim, "A socio-behavioral study of home computer users' intention to practice security," in *Proceedings of the Ninth Pacific Asia Conference on Information Systems*, 2005, pp. 7–10.

[29] S. Milne, S. Orbell, and P. Sheeran, "Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions," *Br. J. Health Psychol.*, vol. 7, no. 2, pp. 163–184, 2002.

[30] G. M. Marakas, R. D. Johnson, and P. F. Clay, "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time.," *J. Assoc. Inf. Syst.*, vol. 8, no. 1, pp. 15–46, Jan. 2007.

[31] A. Bandura, "Self-efficacy: Toward a unifying theory of behavioral change," *Psychol. Rev.*, vol. 84, no. 2, pp. 191–215, 1977.

[32] C. M. Ringle, S. Wende, and J.-M. Becker, "SmartPLS 3. Bönningstedt: SmartPLS," *Retrieved Httpwwwsmartplscom*, 2015.

[33] F. D. Davis, "A Technology Acceptance Model for Testing New End-User Information Systems: Theory and Results," MIT, 1986.

[34] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Q.*, vol. 13, no. 3, pp. 319–340, 1989.

[35] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and recommended remedies.," *J. Appl. Psychol.*, vol. 88, no. 5, p. 879, 2003.

[36] N. K. Malhotra, S. S. Kim, and A. Patil, "Common Method Variance in Is Research: A Comparison of Alternative Approaches and a Reanalysis of past Research," *Manag. Sci.*, vol. 52, no. 12, pp. 1865–1883, Dec. 2006.

[37] J. Hair, W. Black, B. Babin, and R. Anderson, *Multivariate data analysis*, 7th ed. Upper Saddle River, NJ: Prentice Hall, 2010.

[38] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *J. Acad. Mark. Sci.*, pp. 1–21, 2015.