Aug 10th, 12:00 AM

Too Close to Home: The Drivers of Perceived Risk of Home Automation

Sameh Al-Natour
Ryerson University, salnatour@ryerson.ca

Hasan Cavusoglu
University of British Columbia, cavusoglu@sauder.ubc.ca

Arash Saghafi
Tilburg University, a.saghafi@tilburguniversity.edu

Natalia Wiercinska
Signify, natalia.wiercinska@signify.com

Too Close to Home: The Drivers of Perceived Risk of Home Automation

Emergent Research Forum (ERF)

Sameh Al Natour
Ryerson University
salnatour@ryerson.ca

Hasan Cavusoglu
University of British Columbia
cavusoglu@sauder.ubc.ca

Arash Saghafi
Tilburg University
asaghafi@uvt.nl

Natalia Wiercinska
Signify
natalia.wiercinska@signify.com

Abstract

While automation in the workforce is widely studied, home automation, and the accompanied reservations about potential risks and privacy invasion, is deficiently examined and worthy of research attention. Seeking to understand the factors that aggravate the perceived risk of using smart home devices, this study identifies and examines the effects of three types of concerns on perceived use risk. These address the behaviors of the device and its manufacturer, as well the privacy concerns emerging from its use. The results of a survey of current users confirm that product and privacy concerns explain a large portion of the variance in perceived risk, and further suggest that privacy concerns are driven by the uncertainty about what data is collected by the device, and how that data is used and protected. The study makes initial but significant contributions to our understanding of the inhibitors affecting the adoption of these ubiquitous devices.

Keywords

Privacy, home automation, AI, risk.

Introduction

Automation has been a cornerstone of industry as means to improve productivity, reduce costs, and/or induce capital accumulation. With the advancement of technology, machines are now able to organize and execute tasks autonomously, resulting in what has been termed 'smart environments' (Qolomany et al. 2017). These environments rely on intelligent algorithms to analyze and make decisions based on data from many sensors that communicate with other devices over the web (Chew et al. 2017). Due to the increased affordability of advanced technology, intelligent automation has also found its way into the lives of consumers at home (Wang and Siau 2019). Benefits of home automation include tangible gains such as energy savings and increased individual productivity (Chew et al. 2017), as well as intangible outcomes such as convenience, comfort, and security (Gunge and Yalagi 2016).

Higher levels of automation, however, could strain expectations of control that users desire to maintain. This phenomenon, referred to as technology creepiness (Tene and Polonetsky 2013), negatively affects users' attitudes and perceptions. Moreover, the benefits of smart home automation are often attained through the collection and analysis of extensive amounts of data from users' daily behavior (Wang and Siau 2019). Sharing such information with vendors of smart home devices gives rise to privacy and other types of concerns that may negatively affect the intention to these technologies (Al-Natour et al. 2020). The current paper focuses on the latter, and explores the key concerns that influence users' risk tolerance when it comes to home automation, and consequently the incorporation of artificial intelligence (AI) in their daily lives. We report on the findings from a survey of 157 users of smart home devices in an effort to better understand the factors that affect users' privacy concerns, as well as the effects of the latter together with

product and vendor concerns on perceived risk. A better understanding of the antecedents to perceptions of use risk allow for better designs of these devices, and a more accurate appreciation of users' adoption decisions.

Background Literature

Smart home devices are designed to automate the activities that otherwise require human action and intelligence (Alishath et al. 2019). Nowadays, artificially intelligent devices, be they standalone or as a combination of technologies, are present all around the house as water quality monitoring systems, voice assistants, smart security systems, or smart heating that can be controlled and accessed through smartphones, amongst others. In spite of their clear benefits, users of smart home devices perceive the loss of control over the device's operations as creepy (Tene and Polonetsky 2013). A considerable number of users express unease about giving up control, and foresee that as a significant barrier in the context of smart home adoption (Balta-Ozkan et al. 2013).

Along with the need for control over a device's performance, another inhibiting factor is the perceived risk associated with the use of smart devices (Erdem and Swait 2004). Specifically, perceived use risk refers to the perception that actual harm will result as a consequence of using smart home devices (Al-Natour et al., 2020). Klobas et al. (2019) demonstrated that perceived use risk negatively affects perceived control and intention to use smart home devices. This is consistent with prospect theory (Kahneman and Tversky, 1979), which stipulates that users' decision-making processes are more significantly driven by the perceived risk of an action when compared to the perceived benefits of that action.

A major factor attributing to perceptions of use risk is privacy. Privacy uncertainty is a valid consideration with regards to AI-based smart devices (Chew et al. 2017). While significant advances have been made in relation to institutional protections of consumer privacy in many contexts, it is often the case that regulations concerning privacy have to play catch-up when technologies are applied in emerging areas. We view the smart home device as such a context, where consumers understandably experience significant uncertainty in regards to the mechanisms available for the protection of their privacy, and probably more significantly, in relation to what is being done with their personal data. Hence, we propose to investigate the role of that uncertainty and consequent concerns in affecting users' perceptions of the risk associated with smart home device use. These concerns stem from the presence of asymmetric information regarding how their privacy could be encroached (Al-Natour et al., 2020). The technology vendor's characteristics can also affect smart home usage. Jung and Seock (2016) examined users' attitudes toward a product based on positive and negative information about the vendor, and found a direct effect on usage intentions. Similarly, Al-Natour et al. (2020), showed that uncertainty about a mobile app provider can act as an inhibitor to app adoption and increase the perceived risk of using it. Finally, given the inability of a typical user to fully comprehend the device's internal workings, an uncertainty concerning the device itself likely arises, evoking concerns regarding the device's actions and performance.

In summary, while some of the potential concerns associated with smart technologies have been recognized in the literature, there is a lack of attention to how these concerns manifest in the smart home device context. This setting, while sharing many commonalities with others in which smart adaptive technologies are used, is nonetheless unique in its overreliance on AI technologies, often resulting in autonomous action and minimal user control. As a result, users are understandably less involved in the device's functioning, which introduces more uncertainty about its behaviors. Therefore, our goal in this study is to explore the factors affecting the ongoing use concerns by paying a specific attention to the distinct nature of smart home devices, and focusing on current users of these technologies.

Research Model and Hypotheses

The study focuses on examining users' perceived concerns on perceived use risk of smart home devices. These include product concerns, which refers to users' concerns about how the device will continue to perform in the future. Hence, our focus is on the future expectations of the AI-based performance of the device rather than its characteristics or features. This is consistent with Al-Natour et al.'s (2020) finding that uncertainty about a smart technology such as a mobile app after already adopting it, is primarily driven by the uncertainty about its performance rather than its features. We propose that this uncertainty regarding a smart home device's AI-enabled performance will manifest in the form of concerns regarding

the product. Such concerns relating to issues of performance and control have been proposed as a social barrier to device use, and can increase perceived use risks (Balta-Ozkan et al., 2013).

H1: Users' product concerns positively affect their perceived use risk.

Another antecedent of perceived use risk are the concerns regarding the privacy of one's personal data. Anchored in Al-Natour et al.'s (2020) work, we propose that privacy concerns are driven by users' inability to assess how their personal data is maintained when that data is collected by the device or the vendor. In other words, users' uncertainty about their privacy gives rise to privacy-based concerns. Such concerns, which are a by-product of the uncertainty about the device's and the vendor's privacy-related actions, give rise to perceptions of risk associated with using the smart home device. This proposition has found some support in prior research on smart homes, where it was reported that among other proposed dimensions (performance and time), privacy had a significant effect on perceived use risk (Wang et al. 2020).

H2: Users' privacy concerns positively affect their perceived use risk.

An individual's uncertainty regarding how their information is managed does not only concern what data is collected, but also how that data is managed (Malhotra et al. 2004). Similarly, as proposed by Al-Natour et al. (2020), asymmetric information regarding privacy could give rise to privacy uncertainty across three distinct dimensions relating to the collection, use and protection of personal data. When applied to the context of smart home devices, collection uncertainty refers to the difficulty in assessing what information is collected by the smart home device. Similarly, use uncertainty refers to the difficulty in assessing how the information that is collected by the device is used, while protection uncertainty refers to how that data is protected. All of these types of uncertainties give rise to concerns regarding one's privacy.

H3: Uncertainty regarding what data is collected positively affects users' privacy concerns.

H4: Uncertainty regarding how data is used positively affects users' privacy concerns.

H5: Uncertainty regarding how data is protected positively affects users' privacy concerns.

The final hypothesis in our model proposes a direct effect of user's concerns about the vendor on the perceived risks associated with the use of a smart home device. The effects of consumer disposition towards a vendor on their subsequent perceptions and evaluations have found broad support in the literature (Jung and Seock 2016). In technology contexts, concerns about a vendor can stem from the uncertainty regarding their characteristics (such as in auctions), or their opportunistic behavior (Dimoka et al. 2012). Since smart home device users are likely to resolve the uncertainty regarding the seller's characteristics when buying the device, active users' concerns regarding the vendor are anchored in their inability to assess whether the vendor will act opportunistically in the future as they continue to use the device. Such concerns regarding the vendor act as yet another factor contributing to use risk.

H6: Users' vendor concerns positively affect their perceived use risk.

Method

One-hundred fifty-seven respondents recruited from Amazon Mechanical Turk completed a survey about their use of smart home devices. The respondents were members of the MTurk Masters, which is a group consisting of the top of the MTurk marketplace that have been granted special qualification. To inform the structure of the model, eight interviews were conducted with current users of smart home devices. Each interview lasted between 30 and 45 minutes, and due to pandemic restrictions, all interviews were virtual. A Critical Incident Technique was used in the interviews, where participants were asked to recall/describe an experience using the smart home device and elaborate on its impact. Interviewees were also asked about their opinions regarding smart home devices, and were presented with a number of scenarios that describe typical and atypical device behavior and asked to indicate their feelings, concerns, and intentions. Overall, findings from the interviews support the proposed model.

All constructs were measured using 7-point multi-item Likert scales, ranging from "strongly agree" to "strongly disagree". The scale to measure perceived use risk was adapted from Featherman and Pavlou (2003), who developed a scale to measure overall risk of e-service adoption. The scales used to measure the privacy constructs were adapted from Al-Natour et al. (2020). Two new scales were developed to measure product and vendor concerns that were adapted from those developed by Al-Natour et al. (2020) to measure

product and seller uncertainty. Both usage experience (how long has the device been used) and usage frequency were measured using an ordinal scale, and were included in the model as control variables.

Results

Respondents reported on voice-controlled intelligent assistants with a frequency of 38%, followed by smart home security (22%) and home control devices (22%). The sample was 55% male and 38% female, with 7% indicating a non-binary gender or refusing to declare. In term of use frequency, a majority of respondents indicated that they use the smart home device either daily (40%) or multiple times a day (28%). In terms of length of use, 43% indicated that they have been using the device for "7-12 months", 32% indicated "1-3 years", and 18% have been using the device for "more than 3 years".

An assessment of the measurement model and an analysis of the structural model were performed using Partial Least Squares with SmartPLS 3.0 (Ringle et al. 2015). The loadings for all items on their intended constructs exceeded the recommended tolerance of 0.70 (Ringle et al. 2015). In support of discriminant validity, the square root of the average variance extracted (AVE) exceeded any of the bivariate correlations between the constructs (Barclay et al. 1995). The Cronbach's alpha and composite reliability were all above the suggested minimum of 0.70 (Fornell and Larcker 1981).

The results of the structural model largely supported our hypotheses. Consistent with hypothesis 1, perceived product concerns exerted a positive effect on perceived use risk ($\beta = 0.52$, $p < 0.01$). Similarly, consistent with hypothesis 2, perceived privacy concerns increased the perceived use risk ($\beta = 0.30$, $p < 0.01$), while the former was shown to significantly be affected by the three privacy uncertainty dimensions of collection ($\beta = 0.16$, $p < 0.05$), use ($\beta = 0.26$, $p < 0.05$), and protection ($\beta = 0.36$, $p < 0.01$). Thus, hypotheses 3-5 are also supported. Finally, the results revealed that the effects of vendor concerns on perceived use risk are not statistically significant ($\beta = 0.05$, $p > 0.10$). Hence, hypothesis 6 is not supported. Only one of the control variables, namely use frequency, exerted a significant negative effect on perceived use risk ($\beta = -0.13$, $p < 0.05$). Jointly, the variables explained 59% of the variance in perceived risk, while the three privacy uncertainty dimensions explained 52% of the variance in perceived privacy concerns.

Discussion

The results from this study provide general support for the proposed model. The large effect of perceived product concerns signals that the information asymmetry concerning how these devices operate leads to concerns regarding their use, and subsequently risk assessments. Similarly, information asymmetry regarding data collection and the privacy of that data, evokes privacy concerns, and subsequently increases perceived use risk. The results concerning the effects of the three dimensions of privacy uncertainty on overall privacy concerns highlight that overall privacy concerns are not only driven by the uncertainty about what data is being collected by the device, but also how that data is used and protected. The relatively large effects of protection uncertainty on privacy concerns highlights the need to more effectively communicate data protection mechanisms, whether these are a part of the device's functioning or are deployed on the vendor's end. Future research should further investigate the role played by these protection mechanisms in influencing perceived protection uncertainty, and eventually privacy concerns and use risk.

The statistically non-significant effect of vendor concerns on use risk can be explained by the concentrated nature of the smart home device market. The massive majority of respondents reported on devices that are created by reputable large companies. Nonetheless, with the continued proliferation of these devices, and their continued infusion into all aspects of homelife, the number, size and type of devices, and the vendors that offer them are likely to increase in the future. As a result, vendor concerns will likely emerge as a substantial consideration as the market becomes less concentrated. The large proportions of variance explained in the examined constructs indicate the saliency and sufficiency of their determinants. Nonetheless, future research should attempt to identify further determinants to overall use risk, and the effects of that on users' attitude, intentions and actual behavior. Since smart home devices vary in purpose, sophistication, and potential impact, the saliency of the identified antecedents is likely to vary with device type. Hence, future research should examine segments of the smart home device market.

The current study has focused on active users of smart home devices. Future research should explore whether the factors examined in this study are salient and influence the perceptions and the intentions of

non-users. Similarly, future research should investigate the specific technology factors that may enhance adoption and endow users with a clearer understanding of the benefits and risks involved. On the other hand, while the current study sheds some light on some of the factors influencing current users' perceptions of risk, future work should be directed at identifying other risk drivers, and more importantly, the determinants of these drivers, so home automation technology can be designed to mitigate perceived risks.

Conclusion

With an objective of understanding the factors that aggravate the perceived risk of using smart home devices, this study identifies and examines the effects of three types of concerns on perceived use risk. The results of a survey of current users indicate that product and privacy concerns explain a large portion of the variance in perceived risk, and further suggest that privacy concerns are driven by the uncertainty about what data is collected by the device, and how that data is used and protected. The study makes significant contributions to our understanding of the inhibitors affecting the adoption of these ubiquitous devices.

Acknowledgements

The authors would like to thank the Social Sciences and Research Council of Canada and the Tilburg School of Economics and Management for their generous support of this research.

REFERENCES

Al-Natour, S. Cavusoglu, H. Benbasat, I. and Aleem, U. 2020. "An Empirical Investigation of the Antecedents and Consequences of Privacy Uncertainty in the Context of Mobile Apps," *Information Systems Research* (31:4), pp. 1037-1063.

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

Barclay, D. Higgins, C. and Thompson, R. 1995. "The Partial Least Squares Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration," *Technology Studies* (2), pp. 285-324.

Chew, I. Karunatilaka, D. Tan, C. P. and Kalavally, V. 2017. "Smart lighting: The way forward? Reviewing the past to shape the future," *Energy and Buildings* (149), pp. 180-191.

Dimoka, A., Hong, Y., and Pavlou, P. A. 2012. "On Product Uncertainty in Online Markets: Theory and Evidence," *MIS Quarterly* (36:2), pp. 395-A315.

Erdem, T. and Swait, J., 2004. "Brand Credibility, Brand Consideration, and Choice," *Journal of Consumer Research* (31:1), pp. 191-198.

Featherman, M. S. and Pavlou, P. A. 2003. "Predicting e-services adoption: A perceived risk facets perspective," *International Journal of Human-Computer Studies* (59:4), pp. 451-474.

Fornell, C. and Larcker, D. F. 1981. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18), pp. 39-50.

Gunge, V. S. and Yalagi, P. S. 2016. "Smart Home Automation: A Literature Review," *International Journal of Computer Applications* (975), pp. 8887- 8891.

Jung, N. and Seock, Y. 2016. "The impact of corporate reputation on brand attitude and purchase intention," *Fashion and Textiles* (3), pp. 1-15.

Kahneman, D. and Tversky, A. (1979). "Prospect theory: An analysis of decision under risk," *Econometrica* (47:2), pp. 263–292.

Klobas, J. E., McGill, T. and Wang, X. 2019. "How perceived security risk affects intention to use smart home devices: A reasoned action explanation," *Computers & Security* (87), p. 101571.

Malhotra, N. K., Kim, S. S. and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Tene, O. and Polonetsky, J. 2013. "A theory of creepy: Technology, privacy and shifting social norms," *Yale JL & Tech*. (16), p. 59.

Wang, W. and Siau, K. 2019. "Artificial intelligence, machine learning, automation, robotics, future of work and future of humanity" *Journal of Database Management* (30:1), pp. 61-79.

Wang, X., McGill, T. and Klobas, J. 2020. "I Want It Anyway: Consumer Perceptions of Smart Home Devices," *Journal of Computer Information Systems* (60), pp. 437-447.