Privacy-Usefulness Trade(off): Consumer Perceptions of the Information Exchange in the Context of the Internet of Things

Aleksandra Mikhailova
Stockholm School of Economics
Jonas Colliander
Stockholm School of Economics

Cite as:
Mikhailova Aleksandra, Colliander Jonas (2024), Privacy-Usefulness Trade(off): Consumer Perceptions of the Information Exchange in the Context of the Internet of Things. *Proceedings of the European Marketing Academy*, 52nd, (119811)

Paper from the 53rd Annual EMAC Conference, Bucharest, Romania, May 28-31, 2024

Privacy-Usefulness Trade(off): Consumer Perceptions of the Information Exchange in the Context of the Internet of Things

Abstract:

Nowadays the internet has outgrown PCs and mobile devices, integrating into home appliances, symbolizing the emergence of the Internet of Things (IoT). Where the internet thrives, valuable consumer information follows suit. This leads to home appliances equipped with internet connection, sensors, and even cameras, gaining broad access to consumer data, also including insights into intimate aspects of daily life. This nature of the information collected by IoT devices, distinct from conventional online consumer information, presents a novel context for privacy-related research. Results of 2 experimental studies indicate that when IoT devices access intimate consumer information to deliver tailored advertising, it amplifies the perceived usefulness of the device (along with attitudes and intentions), but not privacy concerns. These findings offer novel insights into consumer privacy calculus theory within IoT marketing communications, encouraging future research in this domain.

Keywords: Internet of Things, Privacy, Artificial intelligence

Track: Digital Marketing & Social Media

1. Introduction

Technological development promotes the expansion of the internet far beyond PCs and mobile devices, creating a new paradigm of the Internet of Things (IoT). IoT or "smart" devices are equipped with sensors, software and network connectivity that allow them to collect and exchange data with other devices and systems (IBM, n.d.). However, it is Artificial Intelligence (AI) that empowers IoT devices with cognitive abilities, enabling real-time data analysis and forecasting capabilities. This synergy makes IoT devices truly autonomous (Dupont, 2022), and a powerful instrument for marketing activities (Chui et al., 2023). The consumer sector is projected to lead in the number of connected IoT devices, reaching a global total of 17 billion by 2030 (Vailshery, 2023), which is more than double of the current world population. The growing popularity of IoT devices might stem from their perceived usefulness. For example, studies on the adoption of voice assistants (VAs) reveal that perceived usefulness significantly influences consumers' attitudes toward VAs (Choung et al., 2023). At the same time, research indicate that consumers' privacy concerns are one of the key obstacles to the adoption of IoT devices (De Cremer et al., 2017). However, studies show that consumers, in line with the privacy calculus theory, weigh privacy risks against data-sharing benefits (Dinev & Hart, 2006), and are willing to give out some of their personal information in exchange for, for example, ads personalization (Martin & Murphy, 2017). This suggests a trade-off- sacrificing aspects of privacy in return for receiving something of high usefulness.

However, one core element of the privacy-usefulness trade-off remains rather obscure within the research on IoT and other AI-enabled devices – the sensitivity of the information itself. In fact, Mothersbaugh, Foxx, Beatty, and Wang (2012) suggest that research on the privacy paradox – where consumers express concerns about privacy but then disclose information anyway – overlooks the significance of information sensitivity, highlighting the need for further research in this domain. Here, we assert that information and privacy trade-offs differ between conventional online scenarios such as desktop and mobile online shopping, and the use of IoT devices. IoT devices have access to more consumer data, including, but not limited to, photos of consumer's home environment and intimate details of their daily habits (Guo, 2022). This nature and richness of information gathered by IoT devices compared to standard online consumer information provide a distinct context for privacy-related research, which has not yet been fully addressed by the academic community.

Therefore, through 2 experimental studies, we aim to fill part of this gap by exploring how the level of intimacy and sensitivity of consumer information obtained via IoT devices

impact outcomes of marketing communications through these devices. On the one hand, the more intimate and sensitive details IoT devices have access to, the more accurate and useful their recommendations could be to the consumer. On the other hand, increasing access to intimate and sensitive information is likely to give rise to more privacy concerns in consumers, potentially leading to adverse effects of marketing communications utilizing this information.

2. Theoretical Background and Hypotheses Development

2.1 Personalized advertising using consumers' intimate information

The advancements in the IoT and AI enable highly personalized advertising, leveraging access to intimate and sensitive consumer information for targeted marketing communications. Research in adjacent areas, such as online behavioral advertising, highlights its obvious advantages for advertisers yet underscores the privacy concerns for consumers (Boerman et al., 2017). In a recent study on AI-chatbot personalized ads, researchers discovered that highly privacy-conscious consumers tend to dislike such advertisements (W. J. Kim et al., 2023). At the same time privacy calculus theory, though mostly used to explain online information disclosure, also guides consumer responses to personalized ads (Demmers et al., 2018). In the study of Pitardi and Marriott (2021) some respondents declared their will to be overheard by Alexa, the VA, as it allowed them to receive personalized ads they found useful. Usefulness is one of the well-documented driving powers of why people adopt new technology, while one of the key aspects of perceived usefulness is that technology increases user's performance (Davis, 1989). This stands true for IoT devices: nowadays one can prepare dinner using groceries preordered by the smart fridge, all while cleaning the apartment without even touching the vacuum cleaner. Moreover, in the context of IoT, research indicates that although privacy concerns negatively affect attitudes toward using VAs, the positive influence of perceived usefulness counterbalances this impact (Acikgoz et al., 2023). Here, we suggest that for more tailored IoT devices, usefulness will be a function of the amount of information such devices are granted by the user. The more intimate (and thus sensitive) information the IoT devices can access, the more useful they will be to the consumer in that they can deliver more accurate recommendations. Furthermore, we suggest that the consumer will be appreciative of this. Hence, we hypothesize:

> *H1: Increased access of IoT devices to consumers' intimate private information, and subsequent provision of more accurate recommendations, leads to increased perceptions of the usefulness of the IoT device.*

Moreover, and if H1 holds, we posit that the increased usefulness of the recommendations of an IoT device will lead to more favorable attitudes towards not just the IoT device itself, but also towards the VA embedded within the smart device and towards the company behind the marketing communication. Studies have highlighted that personalization enhances brand attitude by amplifying perceived personal relevance while simultaneously reducing the perceived intrusiveness of the advertisement (De Keyzer et al., 2022). At the same time, in the context of IoT these relations between personalization and attitudes towards all parties involved remain unclear. However, previous studies in the marketing context show that the more useful a technology is perceived to be, the higher the attitudes towards this technology and the companies that use it tend to be (e.g., Alkhowaiter, 2023).

Therefore, we hypothesize:

> *H2: Increased access of IoT devices to consumers' intimate private information, and subsequent provision of more accurate recommendations, leads to increased attitudes towards a) the IoT device b) the voice assistant embedded in the IoT device c) the company advertising through the IoT device.*

If both hypotheses 1 and 2 hold, we also propose that this will lead to increased purchase intention of the products recommended in the marketing communication. Numerous studies have documented the connection between increased brand attitudes and increased purchase intentions (Goldsmith et al., 2000; Ko et al., 2005). Hence, we hypothesize:

> *H3: Increased access of IoT devices to consumers' intimate private information, and subsequent provision of more accurate recommendations, leads to increased purchase intentions of the advertised brand.*

2.2 The impact of information sensitivity

Finally, we also would like to heed the call of Mothersbaugh et al. (2012) and consider the sensitivity of the intimate information. Here, we ask whether information that is highly intimate, and therefore also highly sensitive, will lead to increased feelings of privacy risk and decrease the feelings of usefulness of the IoT device. Nearly any private information can be perceived as "sensitive," depending on various factors like context or individual backgrounds (Quinn, 2021). Research on effects of information sensitivity on personalization of the advertising shows that while consumers find personalized ads beneficial, the use of more sensitive information can evoke feelings of inappropriateness (Bleier and Eisenbeiss, 2015). Moreover, information sensitivity is associated with consumer privacy concerns (Wang & Petrison, 1993). Within the domain of the IoT one of the very few and most recent studies

focuses on the use of VAs indicates that information sensitivity notably influences user privacy concerns and affects their willingness to disclose their private information (Ha et al., 2021). Therefore, we hypothesize:

H4: Access of IoT devices to consumers' highly intimate private information, and subsequent use of it for marketing recommendations, leads to a) increased feelings of privacy risks b) decreased feelings of usefulness of the IoT device.

3. Empirical Study 1

3.1 Design and measures

Study 1 comprises an experiment with between-subjects design with 2 conditions (access to consumers' intimate private information of IoT devices: high vs low). It was designed to test access to intimate private information and not *highly* intimate private information, and thus explores hypotheses 1, 2, and 3. We recruited 335 participants (M_{age_group} = 35-44, 51% female) from online panel company in a Western European country. Participants were randomly assigned and introduced to one of two hypothetical scenarios where they had recently purchased a new IoT device – a Samsung smart fridge– equipped with internet access, a touch screen, and a VA – Alexa by Amazon. In the high intimate information disclosure scenario, however, the smart fridge also featured an inbuilt camera in the main compartment. Participants were informed that this camera could capture images of the fridge's contents, analyze the acquired data, and generate tailored recommendations based on the results of the analysis. The scenarios unfolded with the script of participants interacting with Alexa, the VA, seeking culinary inspiration for making a dessert. Alexa's response varied depending on the scenario: in the high private information disclosure scenario, Alexa's suggestions were based on real-time analysis of the fridge's contents ("After analyzing the contents of your fridge, I suggest making an apple pie."), while in the low intimate private information disclosure scenario, suggestions were made without such analysis ("I suggest making an apple pie."). After providing a recipe for the dessert, Alexa generated a shopping list of the required ingredients. Further, participants were asked if they would be inclined to continue by ordering groceries according to this shopping list online from the recommended grocery retailer (7-point bipolar single-item matrix scale from "definitely not inclined" to "definitely inclined"). Then participants completed a survey. Within this survey, participants shared their evaluations regarding statements concerning their attitude toward the smart fridge (α = .94, 7-point Likert scale, adapted from Pitardi & Marriott, 2021), attitude toward the VA (α = .95, adapted, as previous, from Pitardi & Marriott, 2021), attitude toward the grocery

retailer (α = .96, 7-point bipolar matrix scale, from Puzakova et al., 2013), perceived usefulness of the smart fridge technology (α = .97, 7-point Likert scale, adapted from Jaspers & Pearson, 2022) and privacy concerns (α = .90, 7-point Likert scale, adapted from Mothersbaugh et al., 2012). To conclude the survey, participants were asked to respond to a series of basic demographic questions and the question regarding their perception of the realism of the provided scenario.

3.2 Results

Participants in the high private information disclosure condition indicated higher perception of usefulness (n= 168, M = 4.53, SD = 1.77) of the smart fridge technology compared to the participants of the low private information disclosure group (n= 167, M = 4.17, SD = 1.67; t (333) = 1.90, $p < .05$). Moreover, attitude toward the retailer also varied between the conditions: participants in the high private information disclosure condition (M = 4.54, SD = 1.70) showed a more favorable evaluation of the retailer compared to those in the low private information disclosure condition (M = 4.24, SD = 1.55; t (333) = 1.69, $p < .05$). Attitude toward Alexa, the VA, also differed in between the groups: those in the high private information disclosure condition (M = 4.48, SD = 1.60) demonstrated a more positive attitude toward Alexa, then those in low private information disclosure condition (M = 4.12, SD = 1.72; t (333) = 1.97, $p < .05$). Attitude toward the smart fridge, however, did not show significant difference across the groups (high private information disclosure condition (M = 4.64, SD = 1.67) vs low private information disclosure condition (M = 4.35, SD = 1.69; t (333) = 1.58, $p > .05$)). Participants of the high private information disclosure group demonstrated a higher action intention to order the groceries from the recommended retailer (M = 4.45, SD = 1.94) compared to those in the low private information disclosure condition (M = 4.10, SD = 1.79; t (333) = 1.69, $p < .05$). Importantly, however, there was no significant difference in the privacy concerns between the high private information disclosure condition (M = 4.29, SD = 1.77) and low private information disclosure condition (M = 4.38, SD = 1.72; t (333) = -.46, $p > .05$).

4. Empirical Study 2

4.1 Design and measures

Study 2 is represented by an experiment with between-subjects design with 2 conditions (access to consumers intimate private information of IoT devices: very high vs low). It was designed to test H4. We recruited 359 participants (M_{age_group} = 35-44, 100%

female) from the same company as in study 1. Participants were randomly assigned to one of two conditions featuring hypothetical scenarios, both involving the purchase of a new AI-enabled smart washing machine. Then, depending on the assigned condition, participants were told to imagine a specific laundry task: in the low information sensitivity scenario, the task involved washing pants stained with tomato sauce, while in the very high information sensitivity scenario, the pants were stained with menstrual blood. Further both groups of participants were informed that AI technology determined stain types through comparative analysis of current and previously accessed data and autonomously selected the most suitable washing and drying cycles. Moreover, the participants were presented with two subtly distinct detergent advertisements. In the low information sensitivity scenario, part of the ad read: "…The advanced smart enzymes formula helps to get rid of tomato sauce stains in no time…" At the same time in the high information sensitivity scenario, the advertisement was identical but specified the stain as menstrual blood ("…helps to get rid of menstrual blood stains in no time…"). After being introduced to the scenarios of the experiment, participants completed a survey with the same items as in study 1 (save for the question on privacy risks, which in this study was adapted from Massara et al., 2021; $\alpha = .97$).

4.2 Results

Despite expected significant difference in perceived privacy risks between the very high information sensitivity group (n= 181, M = 4.55, SD = 1.96) and low information sensitivity group (n= 178, M = 4.27, SD = 1.94; t (357) = 1.35, p > .05), no significant difference between the groups was observed. Moreover, no significant difference emerged between very high and low information sensitivity concerning perceived usefulness (M = 4.11, SD = 1.86) and low (M = 3.96, SD = 1.88; t (357) = .74, p > .05). A similar pattern emerged across other variables, no differences were found between groups on either questions regarding attitudes or intentions.

5. Discussion

The results of our research once again showcase complex nature of consumers' perception of privacy. Do consumers have finally fully declared the win of the usefulness over privacy in the privacy calculus scenarios? Our research empirically demonstrates that this might be the case. Our results show that IoT devices access to intimate private information, and the more tailored advertising that they can deliver as a result, increases the perceived usefulness of the devices (and subsequent attitudes and intentions), but not the privacy

concerns. Even when we dial up the level of the intimate information the IoT devices have access to and include highly intimate (and sensitive) information specific to women, there is no significant increase in their perception of privacy risks. This result is notable and partly contradicts existing literature as according to some studies, women in general tend to cherish their personal information more than men (W. Kim et al., 2022). This study, however, though performed with AI-driven technology, took place in a different setting (using IoT device to offer add on services and using personal information to tailor the message). This shows the vastness of the empirical settings in which similar technology is used. And, with results differing from those of our study, demonstrates the probable impact of setting, message, and device. We encourage future researchers in this domain to investigate these aspects further, complementing ours and other studies.

6. References

Acikgoz, F., Perez-Vega, R., Okumus, F., & Stylos, N. (2023). Consumer engagement with AI-powered voice assistants: A behavioral reasoning perspective. *Psychology and Marketing*, *40*(11), 2226–2243.

Alkhowaiter, W. A. (2023). The Role of the Internet of Things Content in Branding: A Framework Designed from the Technology Perspective. *Journal of the Knowledge Economy*.

Bleier, A., & Eisenbeiss, M. (2015). The Importance of Trust for Personalized Online Advertising. *Journal of Retailing*, *91*(3), 390–409.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, *46*(3), 363–376.

Choung, H., David, P., & Ross, A. (2023). Trust in AI and Its Role in the Acceptance of AI Technologies. *International Journal of Human-Computer Interaction*, *39*(9), 1727–1739.

Chui, M., Hazan, E., Roberts, R., Singla, A., Smaje, K., Sukharevsky, A., Yee, L., & Zemmel, R. (2023, June 14). *Economic potential of generative AI*. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier - /. (Last accessed: October 23, 2023)

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly: Management Information Systems*, *13*(3), 319–340.

De Cremer, D., Nguyen, B., & Simkin, L. (2017). The integrity challenge of the Internet-of-Things (IoT): on understanding its dark side. In *Journal of Marketing Management, 33* (1–2), 145–158.

De Keyzer, F., Dens, N., & De Pelsmacker, P. (2022). How and When Personalized Advertising Leads to Brand Attitude, Click, and WOM Intention. *Journal of Advertising*, *51*(1), 39–56.

Demmers, J., van Dolen, W. M., & Weltevreden, J. W. J. (2018). Handling Consumer Messages on Social Networking Sites: Customer Service or Privacy Infringement? *International Journal of Electronic Commerce*, *22*(1), 8–35.

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

Dupont, X. (2022, June 21). *How AI is changing IoT*. https://www.infoworld.com/article/3663017/how-ai-is-changing-iot.html. (Last accessed: November 1, 2023)

Goldsmith, R. E., Lafferty, B. A., & Newell, S. J. (2000). The impact of corporate credibility and celebrity credibility on consumer reaction to advertisements and brands. *Journal of Advertising*, *29*(3), 43–54.

Guo, E. (2022, December 19). *A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook?* MIT Technology Review. https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/amp/. (Last accessed: October 14, 2023)

Ha, Q. A., Chen, J. V., Uy, H. U., & Capistrano, E. P. (2021). Exploring the Privacy Concerns in Using Intelligent Virtual Assistants under Perspectives of Information Sensitivity and Anthropomorphism. *International Journal of Human-Computer Interaction*, *37*(6), 512–527.

Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2021). The Influence of Consumer–Brand Relationship on the Personalized Advertising Privacy Calculus in Social Media. *Journal of Interactive Marketing*, *55*, 16–30.

IBM. (n.d.). *What is the internet of things?* https://www.ibm.com/topics/internet-of-things. (Last accessed: November 2, 2023)

Jaspers, E. D. T., & Pearson, E. (2022). Consumers' acceptance of domestic Internet-of-Things: The role of trust and privacy concerns. *Journal of Business Research*, *142*, 255–265.

Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273–281.

Kim, W. J., Ryoo, Y., Lee, S. Y., & Lee, J. A. (2023). Chatbot Advertising As a Double-Edged Sword: The Roles of Regulatory Focus and Privacy Concerns. *Journal of Advertising*, *52*(4), 504–522.

Kim, W., Park, Y., Shin, J., & Jo, M. (2022). Consumer preference structure of online privacy concerns in an IoT environment. *International Journal of Market Research*, *64*(5), 630–651.

Ko, H., Cho, C. H., & Roberts, M. S. (2005). Internet uses and gratifications: A structural equation model of interactive advertising. *Journal of Advertising*, *34*(2), 57–70.

Lin, J. S. C., & Hsieh, P. L. (2006). The role of technology readiness in customers' perception and adoption of self-service technologies. *International Journal of Service Industry Management*, *17*(5), 497–517.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155.

Massara, F., Raggiotto, F., & Voss, W. G. (2021). Unpacking the privacy paradox of consumers: A psychological perspective. *Psychology and Marketing*, *38*(10), 1814–1827.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. In *Journal of Service Research*, *15*(1), 76–98.

Pitardi, V., & Marriott, H. R. (2021). Alexa, she's not human but… Unveiling the drivers of consumers' trust in voice-based artificial intelligence. *Psychology and Marketing*, *38*(4), 626–642.

Puzakova, M., Kwak, H., & Rocereto, J. F. (2013). When humanizing brands goes wrong: The detrimental effect of brand anthropomorphization amid product wrongdoings. *Journal of Marketing*, *77*(3), 81–100.

Quinn, P. (2021). The Difficulty of Defining Sensitive Data-The Concept of Sensitive Data in the EU Data Protection Framework. *German Law Journal*, *22*(8), 1583–1612.

Vailshery, L. S. (2023, July). *Number of IoT connected devices worldwide 2019-2030*. Statista. https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/. (Last accessed: October 14, 2023)

Wang, P., & Petrison, L. A. (1993). Direct Marketing Activities and Personal Privacy: A consumer Survey. *Journal of Direct Marketing*, *7*(1), 7–19.