International Journal of Marketing Studies; Vol. 13, No. 1; 2021
ISSN 1918-719X E-ISSN 1918-7203
Published by Canadian Center of Science and Education

Correlation Between "Optimal User Experience" Achieved via Extent of User's Private Data Being Shared

Zachary Daniels[1]

[1] Assumption University, Worcester, Massachusetts, USA

Correspondence: Zachary Daniels, Assumption University, Worcester, Massachusetts, USA. E-mail: z.daniels@assumption.edu

Received: January 17, 2021 Accepted: February 19, 2020 Online Published: February 22, 2021

doi:10.5539/ijms.v13n1p63 URL: https://doi.org/10.5539/ijms.v13n1p63

Abstract

Smart Devices have become a fixture in consumers' lives because of their ability to provide consumers with "Optimal User Experiences." However, to provide an "optimal user experience," consumers must give private data to the Smart Devices. The actual sharing of private data is not an issue in consumers' minds, but the private data's potential to be hacked is quite concerning. For example, a consumer's Amazon Alexa Echo could be accessed remotely, and the consumer could be video streamed without their knowledge or consent. The study analyzes the correlations between consumer desire for "Optimal User Experiences" from their Smart Devices and their general perception of sharing their private information to achieve "OUX." The study attempts to determine the foundational aspects of a wide variety of consumer opinions about their risk tolerance by sharing personal data and their desire for the "OUX" in relation to the Smart Devices they utilize regularly.

Keywords: Smart Devices, IoT, IoT privacy, optimal user experience, IoT security

1. Statement of Intended Contribution

The study addresses how much of a correlation exists between Smart Device users and their perception of how much private data they share with brands to have an "Optimal User Experience." The research addresses the question by surveying Smart Device consumers about their use of Smart Devices, how much private data they share with their Smart Devices, and if they are concerned with their Smart Devices being potentially hacked. The research adds to the topic's current knowledge by gaining insight from 154 individuals who own Smart Devices, of varying backgrounds, by utilizing a survey. The closest comparable study asked 11 households and was performed in a qualitative method instead of the quantitative method used in this study.

The attached manuscripts are of value for governmental agencies and policymakers. It highlights that there is a concern for lack of regulation in regards to private data shared with Smart Devices. It is of potential value for brands to better understand consumer perception regarding private data transmitted through IoT to Smart Devices. Suppose Smart Devices can be proactive in actively adjusting consumer perception of private data sharing with brands and the potential of their information possibly being hacked. In that case, brands may prevent overregulation from government entities. Academics can use the findings from this manuscript to determine appropriate follow up studies on the topic; which may focus on how different genders or cultures interpret risk and the optimal user experience.

2. Introduction

Digital marketing has become a pivotal component of integrated marketing communications, which has brought a wealth of data that marketers can utilize and complicated IMC with privacy concerns. "Marketers have come to realize that they can develop better relationships with customers and provide better relationships with customers and provide better, more relevant offers by trapping and analyzing individual-level data," this knowledge has created a great deal of data about each customer. Yet, not all customers appreciate this hyper-personalization (Zahay et al., 2009). As customers begin to understand how much of their private information that they are willingly sharing with marketers, a percentage of customers question why they are "opting in" to share their invaluable data. A recent survey of Americans found "66% do not want behavioral advertising, with three quarters or more rejecting common behavioral advertising practices"; however, these findings come against the modern-day expectations of consumers of wanting personalized experiences in many aspects of their lives

(McDonald & Cranor, 2009). The inconsistency in customer expectations from marketers causes privacy concerns for brands and customers alike.

To maximize digital marketing effectiveness, marketers rely on consumers "opting in" to share their data. It is reasonable to question the potential ramifications if more customers elected not to share their private data. A similar concern would be if digital publishers, such as Google or Facebook, started not to share data with marketers, resulting in marketers reverting to mass marketing instead of niche/ personalized marketing tactics. Even further concerning would be if marketers entirely relied on Google or Facebook to market to their customers. In the event that the publishers elected to stop sharing customer information due to government intervention or their boards' attempt to comply with potentially new government regulations. American marketers can reference the General Data Protection Regulation of Europe, which "created new limits on how companies can collect and share data without user consent" (Satariano, 2020). This regulation could effectively be detrimental to digital marketing if it were to be implemented in America, as it could adversely affect the business model of the primary social media platforms, e-commerce stores, and many search browsers. When considering that digital marketing is a pivotal component of IMC, those mentioned earlier highlight the chain reaction that may arise if consumers stopped sharing their private data with marketers.

As privacy concerns grow in the Internet of Things generation, it is evident that consumers do not entirely understand the privacy agreements that they sign, effectively allowing marketers to utilize personal information for marketing purposes. This issue ranges from mobile apps, television apps, streaming music, ad-blockers, cookies, and more; yet, consumers feel that the marketers are "stealing" their personal information. An area that is not researched well would be privacy concerns and Smart Devices. Consumers "generally choose not to take preventative action to restrict privacy violations; rather, they opt to tolerate the infraction so they can have a better user experience (Aleisa et al., 2020). This conundrum of the consumer feeling that their privacy is violated, yet allowing the violation because it provides a better user experience is the crux of the issue at hand. One would wonder how intrusive can marketers possibly go before the consumer decides that it is too much. If the intrusion continues to improve the "Optimal User Experience," one could postulate that there is no end to the marketer's invasion of privacy.

3. Literature Review

"From a commercial point of view, many IoT objects aim to improve what is known as Quality of Life (Qol), easing people's daily responsibilities" (Anghel et al., 2020). This novel technological advancement is advancing into the desired necessity from the consumer's perspective. "Of the 8.4 billion Smart Devices in the world, more than half are products such as smart TVs and smart audio systems"; however, those particular devices offer the most significant challenges for manufacturers to remedy privacy and security issues (Anghel et al., 2020). As smart products' demand accelerates, manufacturers struggle to prioritize consumers' privacy. The current solution for privacy and security issues lies within blockchain technology, which appears to be a "means of mitigating issues of data security arising in the IoT" (Chanson et al., 2019).

"By dramatically expanding what can be measured and analyzed, digitization is predicted to affect data security issues lives," this innovative shift is based upon the technology found in IoT (Chanson et al., 2019). To best address security and privacy continue upon digitization, manufacturers need to address "confidentiality and integrity of data" that is shared through the interconnected devices" (Chanson et al., 2019). As the versatility of IoT increases with technological advances, "operators will need to establish collaboration with global IoT enablers in developing customized IoT platform architectures relevant to specific industrial verticals" (Tan, 2018). Unfortunately, it has been found that the "requirement has not been addressed due to both market and technology factors" (Yang et al., 2017). This highlights the possibility of creating a standard solution across the IoT to require a significant reduction in IoT growth.

Personalized Disclosures could remedy a push to accelerate the protection of consumer privacy and security concerns in Consumer Law. "Mandated disclosures improve the functioning of markets by helping to overcome information asymmetries without distorting markets by specifying prices, quality, or contracts terms. In contrast, mandated disclosures are a well-suited tool for increasing consumer self-determining and promoting consumer empowerment (Busch, 2016). Essentially, advocating for privacy self-management may be the most effective path towards taking desirable steps towards consumer privacy and security concerns. However, many IoT device security architectures "lack basic security requirements' or "existing security approaches don't exist" (Maxim, n.d.). This highlights privacy self-management implementation if it does not exist consistently.

In the future, security and privacy will need to address the three layers of IoT: "the perceptual extension system, the ubiquitous communication network of heterogeneous integration, and the application and general service" (Liu et

al., 2017). The more interrelated IoT is with consumer life, the more of a challenge governing or limiting its innovation. Policymakers are starting to "debate how to ensure consumer privacy and security without stifling IoT-related innovation." However, the global economic challenge will be creating policy consistent across the world (Waltzman & Shen, 2015). At this particular stage, the FTC can only provide suggestions for IoT manufacturers to implement, many of which would stifle the vertical. As the "policing" of IoT is not reliable at this time, the FTC advocates for "notice and choice: the FTC suggests that a company need not offer a choice to a consumer if the company's expected use is consistent with the context of the interaction" (Waltzman & Shen, 2015).

The root of the issue with IoT is that the "devices are designed for connectivity and integration, not for security, and in many situations, companies neglect even the most basic of security options" (Covington, 2019). The average consumer does not research or understand how much access they are giving to IoT objects; thus, they do not understand the potential issues if they were to be hacked. "Each IoT device is connected to every other device, communicating with one another, transferring and retrieving data, intelligently responding, and triggering actions," if one IoT has a fault, it could adversely affect the vulnerability of all of the interconnected IoT devices (Mena et al., 2018). As manufacturers move forward, "organizations need to more effectively mitigate risks," as there is no universal standard for security and privacy. The responsibility falls on the manufacturer to protect the consumer (Mortleman, 2017).

4. Findings

The literature review determined that there is no significant research that correlates consumer concerns about privacy invasion from IoT. There appears to be a lack of studies asking consumers their general perception of the safety afforded to them from their IoT devices. Policymakers are aware of IoT's possible negative results being infiltrated by hackers due to recent attacks. Yet, the ability to regulate this vertical does not seem feasible at this time. IoT's actual regulation would stifle the innovation and perhaps actually cause a cultural phenomenon to regress at its prime. This does not seem to be a concern of policymakers but is one for developers. As the industry grows and IoT becomes more intertwined with consumer and commercial needs, the innovation can grow without regulation. This may result in a similar issue such as Section 230, where "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider", essentially, IoT may find itself growing at such a rate that the policymakers can not regulate due to sheer size and latitude of implementation (Harmon & Mullin, 2020).

A viable process for developing a universal privacy-setting interface for IoT would be attempting a data-driven design approach. This approach would allow the organizations the opportunity to "develop a layered setting interface" that would enable consumers to determine how much information they want to share based on the association of what percentage of an optimal experience that they would be giving up, to have additional privacy (Bahirat et al., 2018). This approach allows IoT to be regulated with global settings but would not stifle innovation from the niche. This process may provide the solution to privacy and security problems impending in numerous industries. This potential data-driven process would allow for "predicting users' behaviors" so that users would only need to input minimal information to sync their IoT devices (Bahirat et al., 2018). This "simplistic" approach prevents negative consumer experiences that could adversely affect the IoT device manufacturers' success.

Regarding the actual consumer's perception, only one viable literature study was found to detail what the IoT consumer's opinions were of IoT privacy and security. The study looked at a small sample size of "eleven semi-structured homeowners in the United States about their long-term experiences living with IoT devices" (Zheng et al., 2018). The study found that "user assumptions about privacy protections are contingent on their trust of the IoT device manufacturer, users assume giving up privacy is required to fully utilize IoT devices, and users are skeptical of privacy risks from devices that do not record audio or video" (Zheng et al., 2018). The limited findings would seem to put startup companies at a significant disadvantage in the IoT field and provide a path for implementation that would be of least resistance for leery consumers. This information allows for a strong foundation as to what future studies can build upon, better to understand consumer perception of IoT privacy and security risks.

5. Research Method

The research study aims to determine what correlations can be resolved between the consumer and their respective perspective of sharing private data to maximize their "Optimal User Experience" with their Smart Devices in their home.

· Hypothesis 1: Consumers are concerned that their private data may be exploited if their Smart Devices were hacked.

This is a vital topic to analyze regarding marketers, as consumer perception could soon dictate the Smart Device industry's growth. If consumers are very concerned with their private data being hacked, they may opt to request less intrusive Smart Devices. In this situation, users may determine that the "Optimal User Experience" is not worth the potential of their home being compromised by a digital intruder. However, if consumers are not concerned with the possibility of their Smart Devices being hacked, it may signal to manufacturers to continue to push the boundaries to improve the UX.

· Hypothesis 2: Consumers consider "Optimal User Experience or OUX" from Smart Devices to be more critical than the potential for their private data to be potentially hacked from their Smart Devices.

The more marketers understand the relationship between OUX and the potential for hacking, the more they can curate their devices to provide the best experience for their consumers. Brands may pinpoint the tipping point for what is acceptable for brands to do with private data and what is not.

· Hypothesis 3: There is a correlation between a consumer's risk tolerance for the potential of their private data being hacked through their Smart Devices and their education level.

Understanding if the different education level results in more risk aversion, may allow brands to determine better what segments to focus on with their marketing efforts. In theory, this may enable the brands to design more effective integrated marketing campaigns and utilize more productive call to actions in their advertising messaging. The more brands can understand the tipping point for consumers regarding sharing their private data with IoT devices; the more effective their marketing could be. In addition to determining at what point would a brand be unethical in its use of consumer data obtained via an IoT device.

This quantitative study utilizes correlational research, which will help determine the extent of a relationship between the "Optimal User Experience" of the consumer of Smart Devices and their threshold for how much private data they are willing to share with the smart device. There are currently over 45 million smart home devices in the United States; thus, securing a 3% margin of error is not feasible for this preliminary study (2020). As an alternative, the survey asks a balanced percentage of the United States population regarding their income, gender, and age, the following survey questions.

1) Gender: How do you identify?

Man; Non-binary; Woman; Prefer to Self-describe

2) What is your age?

18–24; 25–34; 35–44; 45–54; 55–65; 65–74; 75 to older

3) Which race/ ethnicity describes you?

American Indian; Asian/ Pacific; Black; Hispanic; White; Multiple ethnicities

4) What is your total household income?

Less than $20,000; $20,000 to $34,999; $35,000 to $49,999; $50,000 to $74,999; $75,000 to $99,999; $100,000 to $149,999; $150,000 or more

5) What is the highest school level you have completed or the highest degrees you have received?

Less than high school degree; high school degree; some college; Associate degree; Bachelor degree; graduate degree

6) How many Smart Devices do you own? (Devices in your home that connect to the internet, such as Amazon Alexa, Google Nest Thermostat, Smart TV, iRobot, Amazon Nest, Ring, etc.)

None; 1–3; 4–6; 7–9; More than 10

7) How much "Private Data" do you think you share with your Smart Devices? (Private Data can be categorized as device's location, performance, operating state, and the frequency in which a user is interacting with it, and what way. However, it is not limited to this list.)

A great deal; a lot; a moderate amount; a little; none at all

8) Do you recall agreeing to a privacy agreement with any of your Smart Devices?

Yes; no

9) How valuable to you is your "optimal user experience" from your Smart Devices in your home? (User experience is defined as the overall experience of a product using a product, especially in terms of how easy or please it is to use.)

A great deal; a lot; a moderate amount; a little; none at all

10) Are you concerned with your Smart Devices(s) being hacked and your private data being exploited?

A great deal; a lot; a moderate amount; a little; none at all

11) Is there a threshold for when you think your Smart Device(s) may have too much access to your private data?

Definitely would; probably would; probably would not; definitely would not

The preliminary study that delved into consumer perceptions of IoT privacy and security (Zheng et al., 2018) focused on a small sample size of 11 households. The margin of error regarding the sheer volume of IoT products in the world adversely affects the value of the study as a reference. The current research that is aforementioned achieves a considerable amount of additional validity by capturing insights from an appropriate percentage of the population. This difference in scale would provide direction for future studies to build upon. The study successfully captured input from 154 individuals of varying backgrounds across the United States that had Smart Devices in their home.

6. Results from Study

Hypothesis 1: Consumers are concerned that their private data may be exploited if their Smart Devices were hacked.

> A Spearman's Rho correlation determined a significant correlation between how much data a consumer believes they are sharing and the risk of being hacked, the rs (154) = .219 p = .006. Both variables were ordinal; therefore, a spearman's correlation was used.

Hypothesis 2: Consumers consider "Optimal User Experience" from Smart Devices to be more critical than the potential for their private data to be potentially hacked from their Smart Devices.

> A Spearman's Rho correlation determined a borderline significant correlation between the consumer's "Optimal User Experience" from Smart Devices and their fear of being hacked, the rs (154) = .139, p = .085.

Hypothesis 3: There is a correlation between a consumer's risk tolerance for the potential of their private data being hacked through their Smart Devices and their education level.

> A Spearman's Rho correlation determined no significant correlation between the consumer's education level and their fear of being hacked, the rs (154) = -.032, p = .696.

7. Conclusion

The privacy afforded to consumers who utilize IoT does not translate into consumers' perception of IoT security. The available literature does not extensively analyze the consumer's understanding of what can go wrong if the consumer's IoT devices are infiltrated for nefarious purposes. Consumers have come to expect security from brands merely because they are well known. However, this perception is inaccurate, as examples in this study have highlighted that security lacks many brands at this time. An additional challenge for customers and IoT would be that many brands do not provide clear direction or enforce customers' opportunities to review the security and privacy features for their IoT supported devices. Further research could delve into analyzing what predictors are optimal variables to determine the consumer's "Optimal User Experience." This could include education, income, gender, ethnic background, and quantity of Smart Devices owned by the consumer.

References

Aleisa, N., Renaud, K., & Bongiovanni, I. (2020). The privacy paradox applies to IoT devices too: A Saudi Arabian study. *Computers & Security*, *96*, 101897. https://doi.org/10.1016/j.cose.2020.101897

Anghel, M., Ianc, P., Ileana, M., & Modi, L. (2020). *The Influence of Privacy and Security on the Future of IoT*. Informatica Economică. Retrieved from http://www.revistaie.ase.ro/content/94/04%20-%20anghel,%20ianc,%20ileana,%20modi.pdf

Bahirat, P., He, Y., Menon, A., & Knijnenburg, B. (2018). *A Data-Driven Approach to Developing IoT Privacy-Setting Interfaces*. 23rd International Conference on Intelligent User Interfaces. https://doi.org/10.1145/3172944.3172982

Busch, C. (2016). *Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law*. The University of Chicago Law Review. Retrieved from https://lawreview.uchicago.edu/publication/implementing-personalized-law-personalized-disclosures-consumer-law-and-data-privacy-law

Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E., & Wortmann, F. (2019). Blockchain for the IoT:

Privacy-Preserving Protection of Sensor Data. *Journal of the Association for Information Systems*, *20*(9). https://doi.org/10.17705/1jais.00567

Covington, H. (2019). *Smart Homes: IoT Security and Ethical Concerns*. Northeast Decision Sciences Institute 2019 Annual Conference.

Harmon, E., & Mullin, J. (2020). *Section 230 of the Communications Decency Act*. Electronic Frontier Foundation. Retrieved from https://www.eff.org/issues/cda230

Liu, H., Chen, G., & Huang, Y. (2017). Smart hardware hybrid secure searchable encryption in the cloud with IoT privacy management for a smart home system. *Cluster Computing*, *22*, 1125–1135. https://doi.org/10.1007/s10586-017-1143-6

Maxim, M. (n.d.). *Locking down the IoT*. Telecom Asia. Retrieved from https://www.telecomasia.net/content/locking-down-iot

McDonald, A., & Cranor, L. (2009). *An Empirical Study of How People Perceive Online*. An Empirical Study of How People Perceive Online Behavioral Advertising. Retrieved from https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab09015.pdf

Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective*, *27*(3), 162–182. https://doi.org/10.1080/19393555.2018.1458258

Mortleman, J. (2017, January 9). *Secure IoT before it kills us*. ComputerWeekly.com. Retrieved from https://www.computerweekly.com/feature/Secure-IoT-before-it-kills-us

Satariano, A. (2020, April 27). *Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates*. Retrieved from https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html

Smart Home - United States: Statista Market Forecast. (2020). *Statista*. Retrieved from https://www.statista.com/outlook/279/109/smart-home/united-states

Tan, D. (2018). *2018-traversing the digital wave*. Telecom Asia. Retrieved from https://www.telecomasia.net/content/2018-traversing-digital-wave

Waltzman, H., & Shen, L. (2015). *The Internet of Things - Mayer Brown*. Retrieved from https://www.mayerbrown.com/en/perspectives-events/publications/2015/07/the-internet-of-things

Yang, C., Lan, S., Shen, W., Huang, G., Wang, X., & Lin, T. (2017). Towards product customization and personalization in IoT-enabled cloud manufacturing. *Cluster Computing*, *20*, 1717–1730. https://doi.org/10.1007/s10586-017-0767-x

Zahay, D., Mason, C., & Schibrowsky, J. O. (2009). (PDF) *The Present and Future of IMC and Database Marketing*. Retrieved from https://www.researchgate.net/publication/235326231_The_Present_and_Future_of_IMC_and_Database_Marketing

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). *User perceptions of smart home IoT privacy*. Proceedings of the ACM on Human-Computer Interaction. Princeton University. https://doi.org/10.1145/3274469