Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 14, No. 1, 2024

The Relationship between Privacy Invasion of Smart Services and Consumers' Intention to Use

Yiqin Wang

School of Economics and Management, Chongqing University of Posts and Telecommunications, Chongqing 400000, China

Abstract: While the wide application of smart technology in services brings efficiency and convenience to consumers, it also can't avoid bringing some negative impacts. Nowadays, the problem of privacy invasion raises concerns about the issues of smart services and directly affects consumers' attitudes towards the use of smart services. This study aims to explore the impact of privacy invasion in smart services on consumers' intention to use them. The results of the study emphasize that privacy invasion has a significant negative impact on consumers' intention to use smart services. The conclusions of the study play a theoretical role for enterprises to grasp the psychology of smart service consumers and improve the mode and process of smart services.

Keywords: Smart Service; Privacy Invasion; Intention to Use.

1. Introduction

The continuous evolution of technologies from computational intelligence to perceptual intelligence to cognitive intelligence has led companies to actively integrate different types of AI into product (including tangible and intangible services) marketing activities [1]. The chatbot market is expected to grow at a rate of 29. 7% per year and reach a further $125 million by 2025, at a CAGR of 24. 3% [2]. Artificial intelligence (AI)-based digital assistants have also accelerated in recent years, with nearly 3. 25 billion voice assistants active across services in 2019 and predictions that this number will surpass the 8 billion mark by 2025 [3]. For the service industry, these shifts will profoundly change service marketing strategies, business models and customer behavior.

However, the development and deployment of smart services raises numerous challenges associated with it. Due to its data-centric nature, privacy has become a central issue in the age of AI [4]. Like Amazon and Google, Apple hires outside contractors to listen to user recordings of its voice assistant service, which often include medical information, private conversations, and financial transactions, in addition to user data showing location, contact, and app data, according to The Guardian. China Consumers' Association released the "100 App Personal Information Collection and Privacy Policy Evaluation Report", which shows that the 10 types of apps evaluated are generally suspected of over-collecting personal information, of which 59 apps are suspected of over-collecting location information, and 28 apps are suspected of over-collecting address book information. Privacy concerns caused by smart services have become ubiquitous, making it difficult for consumers to control when, how, and to what extent their personal information is accessed. According to a report by Microsoft Bing Ads, 41 percent of respondents said they don't trust digital assistants, believing they compromise privacy through passive listening. In addition, about 52% said they were concerned that their personal information was not secure [5]. It can be seen that while smart services have become the mainstream of the consumer market, the privacy issues have become more and more complex. The privacy invasion of consumers has caused serious negative effects on their psychology and behavior, and is not conducive to the development of the industry.

At present, most scholars study the psychological reaction of consumers in the face of data leakage based on the privacy calculus theory or social contract theory, or explore the privacy risk of smart services based on the personalization-privacy paradox and technology acceptance model. However, there are few studies on the overall path of consumer negative experience caused by privacy invasion of smart services is still unclear. The complex challenges faced by smart services still require more detailed research in academia.

In view of the above phenomena, this paper introduces the conservation of resources theory. Conservation of resources theory is a kind of stress theory. Resource consumption, exposure to threats and reduced returns on investment can all have a negative impact on an individual's physical and mental health, resulting in negative outcomes such as burnout. Privacy is a very valuable resource [6], and invasion of privacy is a consumption of resources.

Based on this, this study is based on exploring the specific impacts of privacy invasion on consumer psychology and behavior in the context of the rapid development of smart services and the increasingly unavoidable invasion of consumer privacy by service providers.

2. Theoretical Framework

2.1. Conservation of resources (COR) theory

The conservation of resources (COR) theory is one of the most cited theories in organizational behavior research in the past 30 years, providing important theoretical support for explaining organizational psychology and behavioral phenomena [7]. The underlying assumption of COR theory is that people are always actively working to maintain, protect, and build what they perceive to be valuable resources; the potential or actual loss of these resources is a threat to them. Stress occurs when central or critical resources are threatened with loss. Resources are the central concept of this theory and are defined as things that are valuable to an individual's survival and development. COR theory suggests that negative outcomes such as burnout occur when individuals invest large amounts of inherent resources, such as time, energy, opportunities, and social connections, and receive negligible

resources in return .

COR theory emphasizes the preponderance of resource loss. The effects of resource gains and losses are asymmetric, with resource losses having a greater impact on individual behavior change. COR theory explains the mechanisms of burnout, stress, and performance primarily in terms of an individual's resource input-output imbalance. As a motivational theory, conservation of resources (COR) theory broadly predicts people's motivations and behaviors [8]. For example, consumers may eventually become fatigued by their excessive purchase-related cognitive dissonance [9], and overexposure to an experience, technology, interface, or stimulus can also saturate them with stress [10]. So, consumers may feel pressured when privacy as a valuable resource is threatened in smart services. Although the introduction of AI technology into service scenarios has promoted service efficiency to a certain extent, brought a sense of novelty to consumers, and can supplement consumers' psychological resources in the short term, the negative impact of AI technology on privacy on consumers is much more far-reaching, and the consumption of psychological resources may eventually exceed the benefits.

2.2. Negative Impact of privacy invasion on consumers' intention to use

Privacy as a legal, sociological, and economic concept has been widely studied in several academic fields [11]. As an untouchable right and a valuable resource, it can generally be categorized into two types: physical privacy and information privacy. This paper focuses on informational privacy, which can essentially be defined as the ability of people to control when, how, and to what extent they access personal information. And invasion of privacy can be seen as a violation of norms [12].

According to COR theory, people will actively acquire, maintain, or protect resources they recognize as valuable. Privacy as a valuable resource in smart services essentially corresponds to the threat of resource loss due to the unpredictability of advanced technologies, low transparency of algorithms, lack of humanity, and lack of clarity, triggering consumer concerns [13].For example, consumers are concerned about chatbots sharing collected and stored data to the cloud [1], and voice shopping services provided by smart speakers involving consumer privacy transactions between manufacturers and third parties. Privacy invasions occur when businesses collect or use personal information without the informed and voluntary consent of individuals. Privacy invasions range in severity from unsolicited spam to identity theft, with serious adverse effects on consumer resource protection. The current literature suggests that privacy issues can induce reactive cognition and behavior [14], including: purchasing behavior [15], intention to communicate online [16], technology adoption [17], and customer satisfaction [18]. It also leads to the development of discontinuous use and conversion intentions [19]. In smart services, more consumer personal information is collected and recorded unconsciously, seamlessly, and continuously [20]. These privacy issues affect consumers' perceptions of intrusiveness, uncertainty, and risk, which can affect their intention to use.

In summary, in smart services, service providers usually transform consumer behavior data into effective information in order to create a more valuable consumer experience. However, due to the large amount of data collected and shared, the increasing diversity of service providers, and the growing complexity, there is an unavoidable negative experience of privacy invasion in the use of smart services by consumers. Although there are varying degrees of consumer attention to privacy invasion under smart services in the context of technological dependence and cognitive differences, such a negative experience will undoubtedly affect the subsequent behavioral intentions of consumers thereby constraining the development of the industry. With low privacy invasion, a person is essentially able to fully control the access of smart service devices to self-relevant information, and smart services can have a positive impact on consumers, who are willing to use and experience the new technology .Conversely, in the case of high privacy invasion, a person cannot control the smart service's access to self-relevant information, and the consumer's use of the smart service is perceived to be a privacy-intrusive behavior of the smart service product thereby reducing the consumer's intention to use it. Therefore hypothesis one is proposed;

Hypothesis I: Consumers' intention to use smart services is lower in high privacy invasion situations.

3. Research Findings and Theoretical Contributions

This article argues for the negative impact of privacy invasion on consumers' intetion to use based on the COR theory. This paper introduces COR theory into the research field of negative experience caused by smart services, regards privacy as a valuable resource, and improves the theoretical research on the impact of privacy invasion on consumer behavior. Much of the previous research on privacy invasion has focused on the privacy protection, privacy risk dimension [22]; Consumer-oriented research has focused on the area of personal control [23].Focusing on the privacy invasion of smart services, this paper examines the process by which resources interact between individuals and social environments, and explores consumers' psychological responses and behavioral reactions when confronted with privacy invasion. Provides a new interpretive perspective on reduced consumer intention to use.

4. Research Limitations and Future Directions

In this paper, we only consider the negative effects due to privacy invasion in smart services, and we need to study the negative effects in more smart service scenarios in the future. For example, information overload and algorithm aversion caused by the development of advanced technology. In the case of smart services, it is also possible to focus on other elements, such as the Valley of Terror effect due to the level of intelligence of service robots or other explanatory studies of the negative effects of smart services. In addition to this other driving mechanisms that may produce negative effects can also be investigated.

References

[1] Song, M., Xing, X., Duan, Y., Cohen, J., & Mou, J. (2022). Will artificial intelligence replace human customer service? The impact of communication quality and privacy risks on adoption intention. Journal of Retailing and Consumer Services, 66, 102900.

[2] Pantano E, Pizzi G. Forecasting artificial intelligence on online customer assistance: Evidence from chatbot patents analysis[J]. Journal of Retailing and Consumer Services, 2020, 55: 102096.

[3] Malodia, S., Islam, N., Kaur, P., & Dhir, A. (2021). Why do people use Artificial Intelligence (AI)-enabled voice assistants?. IEEE Transactions on Engineering Management, 71, 491-505.

[4] Du, S., & Xie, C. (2021). Paradoxes of artificial intelligence in consumer markets: Ethical challenges and opportunities. Journal of Business Research, 129, 961-974.

[5] Olson, C., & Kemery, K. (2019). 2019 Voice report: Consumer adoption of voice technology and digital assistants. Retrieved from https://about.ads.microsoft.com/enus/insights/2019-voice-report

[6] Whitman, M. V., Halbesleben, J. R., & Holmes IV, O. (2014). Abusive supervision and feedback avoidance: The mediating role of emotional exhaustion. Journal of organizational behavior, 35(1), 38-53.

[7] Freedy, J. R., & Hobfoll, S. E. (1994). Stress inoculation for reduction of burnout: A conservation of resources approach. Anxiety, Stress & Coping, 6(4), 311–325.

[8] Chen, S., Westman, M., & Hobfoll, S. E. (2015). The commerce and crossover of resources: Resource conservation in the service of resilience. Stress and Health, 31(2), 95-105.

[9] Menasco, M. B., & Hawkins, D. I. (1978). A field test of the relationship between cognitive dissonance and state anxiety. Journal of Marketing Research, 15(4), 650-655.

[10] Haenlein, M., Huang, M. H., & Kaplan, A. (2022). Guest editorial: Business ethics in the era of artificial intelligence. Journal of Business Ethics, 178(4), 867-869.

[11] Wang, L., Sun, Z., Dai, X., Zhang, Y., & Hu, H. H. (2019). Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. Information Technology & People, 32(6), 1679-1703.

[12] Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life.Palo Alto, CA: Stanford University Press.

[13] Zarifis, A., Kawalek, P., & Azadegan, A. (2021). Evaluating if trust and personal information privacy concerns are barriers to using health insurance that explicitly utilizes AI. Journal of Internet Commerce, 20(1), 66-83.

[14] Xu, Y., Zeng, Q., Wang, G., Zhang, C., Ren, J., & Zhang, Y. (2020). An efficient privacy-enhanced attribute-based access control mechanism. Concurrency and Computation: Practice and Experience, 32(5), e5556.

[15] D'Souza, G., & Phelps, J. E. (2009). The privacy paradox: The case of secondary disclosure. Review of Marketing Science, 7(1).

[16] Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of interactive marketing, 18(3), 15-29.

[17] Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. MIS quarterly, 339-370.

[18] Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. Journal of business research, 59(8), 877-886.

[19] Wang, L., Sun, Z., Dai, X., Zhang, Y., & Hu, H. H. (2019). Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. Information Technology & People, 32(6), 1679-1703.

[20] Lee, D., & Park, N. (2021). Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. Multimedia Tools and Applications, 80(26), 34517-34534.

[21] Aminizadeh, S., Heidari, A., Toumaj, S., Darbandi, M., Navimipour, N. J., Rezaei, M., ... & Unal, M. (2023). The applications of machine learning techniques in medical data processing based on distributed computing and the Internet of Things. Computer methods and programs in biomedicine, 107745.

[22] Willems, J., Schmid, M. J., Vanderelst, D., Vogel, D., & Ebinger, F. (2023). AI-driven public services and the privacy paradox: do citizens really care about their privacy?. Public Management Review, 25(11), 2116-2134.

[23] Li, C., Dong, M., Xin, X., Li, J., Chen, X. B., & Ota, K. (2023). Efficient privacy-preserving in IoMT with blockchain and lightweight secret sharing. IEEE Internet of Things Journal.