Proceedings of the 5th International Conference on Education Innovation and Philosophical Inquiries
DOI: 10.54254/2753-7048/56/20241631

Exploring the Contradiction Between Convenience and Privacy in Balanced Recommendation System

Yufan Xi[1,a,*]

[1]*Institute of Accounting, Tianjin University of Commerce, Tianjin, 300134, China*
a. 1807060213@stu.hrbust.edu.cn
**corresponding author*

Abstract: Not only does the widespread use of recommendation systems provide consumers with a convenient experience, but it also raises the possibility of a breach of their privacy. As a result, this research makes use of a questionnaire survey to investigate the problem of privacy disclosure and investigate different approaches that can be utilized to resolve the conflict that exists between convenience and privacy. This research investigates the causes from three different points of view: the inadequacy of rules and regulations, variances in the cognitive capacities of customers, and the misuse of data. In addition, the report proposes actions that can be taken to enhance legislation and regulations, improve the cognitive capacity of customers, and prevent the misuse of data. It is beneficial for the maintenance of society harmony and stability to provide assistance to consumers, corporations, and governments in the management of the tension between being convenient and keeping privacy.

Keywords: Recommendation Systems, Privacy, Laws and Regulations, Cognitive Levels

1. Introduction

1.1. Research Background

With the rapid development of global information technology, various social media platforms have given people more ways to obtain information. However, in the process of people's use, the application of the recommendation system is also collecting users' personal privacy information. In the process of using the personalized recommendation service of the recommendation systems, people may give up their privacy for convenience or inadvertently give up their privacy without autonomy, resulting in a contradiction between convenience and privacy. The recommendation system is an intelligent platform that relies on large-scale data mining. According to the user's personal information and item characteristics, the model is established by using statistical analysis, machine learning, and artificial intelligence to predict the user's preference for new items so as to recommend potential items that may get the attention of the users in order to realize personalized information service and decision support [1]. Verizon released the Data Breach Investigations Report in 2022, revealing that over half of the leaked data is personal information [2].

Information that involves individuals or organizations, whether directly or indirectly, falls under the category of data privacy. The processes of data collection, data storage, data query and analysis,

DOI: 10.54254/2753-7048/56/20241631

and data release should not disclose this information and must safeguard it. It also refers to the ability to protect data privacy.

Recently, the related work on privacy protection recommendation systems has mainly been based on federated learning. Federated learning combines the encryption and fuzzing algorithms to enhance privacy protection. In the past, researchers have looked into how to make recommendation systems more private. They used a lightweight privacy protection structure and correctness verification of recommendation results to figure out how to get good results while still keeping users' privacy safe [1]. For instance, researchers have used federated learning as their research object, training the model on edge devices to enhance personalized recommendations and safeguard personal privacy [3]. Some researchers have also looked into the joint matrix factorization problem in recommendation systems that protect privacy and come up with a user-level distributed matrix factorization framework to use federated learning theory and methodology to protect model privacy and value privacy [4].

1.2. Research Gap

Although there are many studies on the data privacy problem of the recommendation system, there is a certain gap in the research on the causes of the problem and reasonable improvement measures from the perspective of consumers. Therefore, it is an important topic to study the contradiction between convenience and privacy in the use of recommendation systems from the perspective of consumers. How to solve the problem of consumer data privacy breaches in the recommendation system?

By investigating a solution to this challenge, the conflict between convenience and privacy in recommendation systems can be better balanced. Given the benefits and drawbacks of existing recommendation systems, as well as limits in consumer privacy protection, acceptable recommendations will be made for recommendation system technology and platform development. Simultaneously, it will provide appropriate recommendations for enhancing data security laws and regulations.

1.3. Fill the Gap

Based on the aforementioned study issues, this paper will begin by providing a comprehensive overview of consumers' cognitive states with respect to recommendation systems and data privacy. Furthermore, it will investigate the phenomenon's underlying factors using theoretical expertise, a questionnaire survey, and data analysis. Ultimately, this paper will propose logical recommendations for the recommendation system, social media platform, and country based on the analysis conducted.

2. Case Description

To produce appropriate suggestion results, the recommendation system will collect a huge amount of user behavior data. In general, the more data collected, the better the knowledge of users and recommended material, as well as the accuracy of the recommendation effect [5]. However, there is a possibility of data compromise. Data breaches are the illegal or inappropriate disclosure of sensitive data or information [6]. Data breaches can occur on both networked and physical devices, such as computers, servers, databases, storage devices, and mobile devices [6]. Data breaches can involve the following sorts of data: personally identifiable information, medical records, credit card and financial information, company secrets, and government secrets [6]. Common causes include network attacks, vulnerable third-party vendors, social media, software vulnerabilities, and employee malfeasance [6]. Privacy breaches in the recommendation system, for example, can result in the information cocoon effect, financial and identity dangers, data abuse, and consumer psychological dislike.

A total of 122 and 103 valid questionnaires were gathered, respectively. Respondents are largely divided into two age groups: 18–29 years old and 30-49 years old. Among them, the proportion of

DOI: 10.54254/2753-7048/56/20241631

those aged 18 to 29 is the largest, reaching 50%. Employees are the largest occupational group among respondents, accounting for 45%, followed by freelancers and students. According to Figure 1, the survey discovered that customers have poor knowledge of data protection, which can lead to discontent and confusion when using social software. At the same time, consumers face evident trade-offs between privacy and convenience.

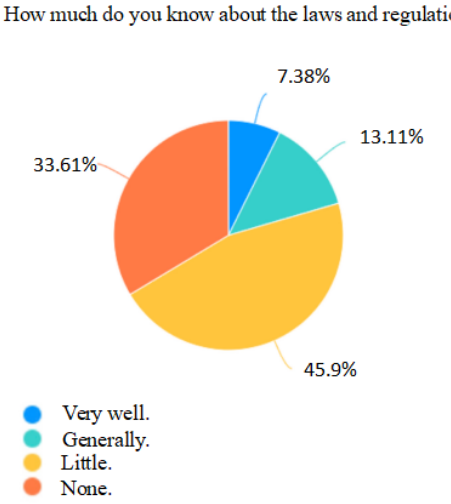

Figure 1: Consumers' Cognition of the Laws of Data Privacy

(Data Sources: original)

When using the recommendation system from Figure 2, over 74% of respondents paid close attention to the preservation of personal privacy, and 99% of respondents reported a conflict between convenience and privacy, according to Figure 3.

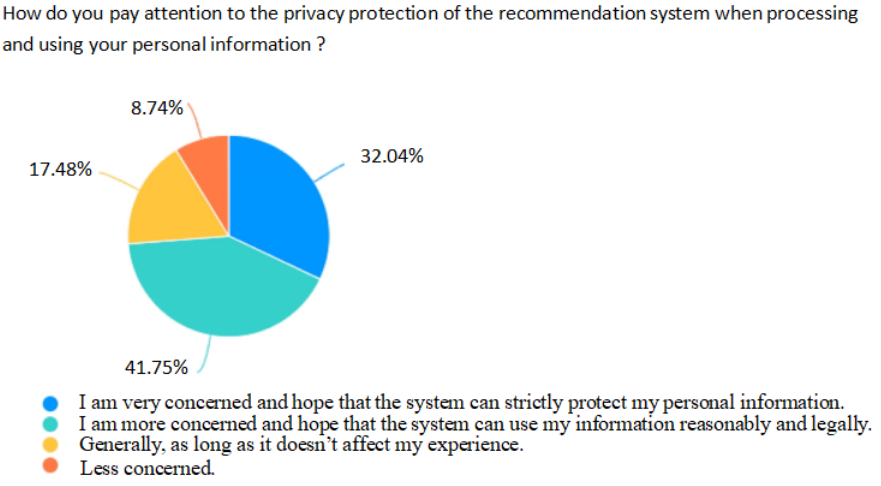

Figure 2: Consumers' Awareness of Privacy Protection

(Data Sources: original)

DOI: 10.54254/2753-7048/56/20241631

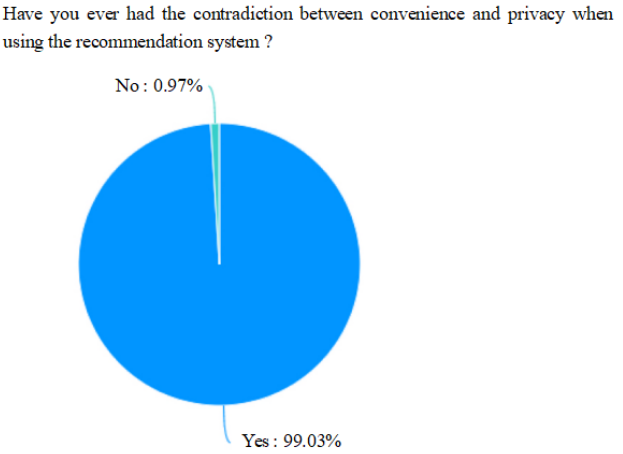

Figure 3: The Ambivalence of Consumers when Using the Recommendation System

(Data Sources: original)

3. Analysis on the Problems

3.1. Reasons for the Imperfection of Laws and Regulations

One of the causes of the conflict between convenience and privacy when utilizing the recommendation system is China's poor data privacy laws and regulations. The recommendation system's individualized service has created new legal obstacles to personal privacy. Determining whether consumers' individualized recommendations unduly violate their personal privacy is a critical issue. Furthermore, the ongoing refinement of the recommendation system makes the process of obtaining personal data more concealed and convenient, increasing the challenge of maintaining personal privacy. China's current "Personal Privacy Protection Law" and other data privacy rules and regulations include fundamental provisions for preserving personal privacy and standardizing data processing. However, these laws and regulations remain unclear about data security duties, levels of protection, and law enforcement. At the same time, due to the disparities in personal information protection standards among laws and regulations, the actual implementation will be fraught with misunderstanding and controversy.

Numerous articles have illustrated the detrimental effects of inadequate laws and regulations. In response to the problem of not enough legal protection for personal privacy in China, Zhao Qin looked at international privacy protection laws and practices. He also looked into how privacy-related legal issues and protection recommendations have changed in the big data era [7]. The implementation mechanism lacks effectiveness, making it challenging for consumers to effectively address instances of personal privacy infringement [7]. In the research on APP privacy security and protection strategy, Li Jun proposed that APP over-collects user privacy and shares illegally acquired data with third-party institutions to gain interest [8]. China’s regulatory authorities at all levels are increasingly cracking down on violations of personal privacy information [8]. Effective implementation of the security and compliance assessment of personal information is lacking, leading to serious data security compliance issues in APP applications [8].

DOI: 10.54254/2753-7048/56/20241631

3.2. Reasons for Differences in Consumers' Cognitive Levels

The disparity in consumers' cognitive levels of data privacy is one of the causes of the conflict between convenience and privacy when utilizing the recommendation system. Consumers' cognitive levels vary based on their awareness of privacy protection, sensitivity to breaches, and attitude toward tailored services. Because people have different levels of cognitive ability, high-cognitive consumers are more likely to accept the recommendation system's collection of user data for the purpose of providing personalized services than low-cognitive consumers. Their acceptance is comparatively higher, allowing for a better balance of privacy and convenience.

Previous papers have demonstrated the impact that customers' cognitive differences in data privacy can have. Researchers developed the social media users' privacy concern model, social cognitive theory, and planned behavior theory [9]. Researchers classify cognitive privacy concerns as low, moderate, indifferent, or high using a questionnaire survey and potential profile analysis [9]. There are cognitive variations among social media users in terms of their privacy concerns.

3.3. Reasons for Data Abuse

The recommendation system's disclosure and abuse of users' personal information is one of the reasons for the contradiction between convenience and privacy when using it. In the era of big data, social media platforms collect users' personal information to generate user behavior portraits and provide personalized recommendation services. However, if these data lack adequate protection, there is a risk of abuse. Users may manipulate their willingness to consume, sell this data to advertisers or other institutions for benefits, and jeopardize the public's personal privacy.

This opinion was supported by Liu Shufeng and other scholars who examined data security risks in the big data and artificial intelligence eras [10]. The security of personal information data is at risk due to the rise in cybercrimes like phishing and hacking brought on by the advancement of Internet technology [10]. Furthermore, machine learning algorithms are capable of analyzing financial information, economic capacities, personal preferences, and other data, after which they can sell advertisements to people or engage in other illicit or commercial activities [10]. Shi Min further noted that abuse of large models and personalized generating services presents new privacy protection issues in the research of data privacy protection of large language models. When offering personalized services, the large model may reveal consumers' interests and consumption patterns. Targeted advertising or even malicious use of it could harm customers [11].

4. Suggestions

4.1. Suggestions on Imperfection of Laws and Regulations

Based on the preceding study, it may be concluded that only stricter legislation will effectively resolve the tension between convenience and privacy in recommendation systems. As a result, this paper recommends that the appropriate government departments conduct a safety and compliance audit of personal information, strengthen laws and rules governing personal privacy, and add to and amend legal provisions that do not make sense to everyone. This would help to avoid disagreements that arise between customers and recommendation systems due to ambiguous legal rules. Furthermore, relevant government departments must standardize privacy risk management for open data sharing in order to properly execute privacy risk assessment and control and establish a balance between convenience and privacy.

Many earlier publications can substantiate the aforesaid suggestions. Meng Xue and other researchers developed a privacy risk management method for open data sharing based on the British experience survey, which effectively validates the usefulness of privacy risk management for open

DOI: 10.54254/2753-7048/56/20241631

data sharing [12]. The Information Commissioner's Office has developed Data Sharing: A Code of Practice, which establishes the principles of accountability, transparency, and fairness, as well as clarifies the responsibilities and obligations of various departments, in order to significantly improve the level of personal data protection in the UK [12].

4.2. Suggestions on Differences in Consumers' Cognitive Level

For the second reason in the preceding analysis, this paper concludes that the higher the level of consumer awareness of privacy concerns, the more rational and objective the recommendation system's attitude toward collecting user data to provide personalized services, and the better balanced the contradiction between convenience and privacy according to their own situation. As a result, this report suggests that researchers from various disciplines collaborate to raise consumer understanding of data privacy. The government should regularly undertake security awareness and education, publicly interpret data privacy rules and regulations, and educate the public on data leakage mitigation measures and personal information protection. At the same time, people need to be encouraged to participate in privacy protection monitoring and review. Social media platforms should enhance customer education on privacy policies and settings, and clearly explain the use of their personal data. Furthermore, social media platforms can incorporate precise privacy control options that empower users to determine the sharing and use of their personal information. Consumers should also take the initiative to study data privacy, pay attention to data leakage incidents, master privacy protection techniques, and develop their cognitive abilities.

Previous articles support the above suggestions. Yang and his colleagues looked at the policies and practices in ten countries and found that because privacy management issues are so complicated, broad, and open to many different interpretations, it is important to set up a government-led, multi-agent collaborative model that includes everyone who needs to be involved [13]. When citizens' digital literacy improves and they have a certain level of risk prevention awareness and privacy protection ability, they can then cooperate and supervise personal privacy protection work in the government's open data to build a long-term, stable, and secure data-open environment and improve the effectiveness of personal privacy protection [13].

4.3. Suggestions for Reasons for Data Abuse

According to the examination of the third reason, the recommendation system can improve the balance between convenience and privacy by preventing data exploitation. As a result, this paper proposes that social media platforms improve the technical optimization of the recommendation system by combining federal learning, data anonymization, data encryption, and differential privacy technology for technological innovation in order to protect consumers' rights and interests while optimizing personalized recommendation services. At the same time, this paper will improve risk assessment management and event response activities, give users with risk warning recommendations, enable users to defend personal privacy in a timely way, and reduce the harm caused by data abuse to consumers.

Previous articles support the aforementioned proposals. In their study Difficulties and Explorations in Data Privacy Protection for Large Language Models, researchers offered several anonymization and data encryption strategies for different stages in response to the challenges of big data privacy protection [11]. Researchers employ differential privacy technology during the training phase and homomorphic encryption technology during the data processing phase. Federated learning is a distributed learning architecture that efficiently balances convenience and privacy, ensuring data privacy [11].

DOI: 10.54254/2753-7048/56/20241631

5. Conclusion

Given the widespread use of personalized recommendation systems on various social media platforms, this paper examines the conflicts between convenience and privacy when consumers utilize these systems and proposes practical solutions. In order to solve this problem, this paper uses a case description to conduct a questionnaire survey and analyze consumer data privacy protection. The analysis results showed that most respondents lack knowledge of data privacy protection, and there is a clear contradiction between convenience and privacy when using the recommendation system for personalized services. Based on the survey results, this paper analyzed the reasons from three perspectives: laws and regulations, consumer cognition levels, and data abuse. It then proposed recommendations for enhancing laws and regulations, raising consumer cognition levels, and reducing data abuse.

This paper examined the literature on privacy protection and recommendation systems, emphasizing the need to strike a balance between convenience and privacy in the big data era. It is conducive to strengthening information leakage management in laws and regulations, increasing consumer awareness and data use, and optimizing the recommendation system. At the same time, it is beneficial to individuals, enterprises, and governments to balance the contradiction between convenience and privacy, reduce disputes, and promote the harmonious development of society.

This article also has some shortcomings. This paper focuses its data sources on the population aged 20 to 50 years old, conducting a cross-sectional study over a specific time period. The study disregards the comparison of other age groups and different time periods. Follow-up research can further increase the population of other age groups and compare and analyze the situation in different time periods.

References

[1] *Zhou, J., Dong, X.L., and Cao, Z.F. (2019) Research Progress of Privacy Protection in Recommendation Systems. Computer Research and Development (10), 2033-2048.*

[2] *Timo, B. (2022) Ransomware Threat Rises: Verizon 2022 Data Breach Investigations Report. Ransomware threat rises: Verizon 2022 Data Breach Investigations Report | News Release | Verizon.*

[3] *Amir, J., Marco, S., Catalin, C., and Michael, S. (2019) A Simple and Efficient Federated Recommender System. In Proceedings of the 6th IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT '19). Association for Computing Machinery, New York, NY, USA, 53-58.*

[4] *Du, Y.J., Zhou,D.Y., Xie, Y., Shi,J., and Gong, M.J.(2021) Federated Matrix Factorization for Privacy-Preserving Recommendation Systems. Applied Soft Computing. Volume 111.2021.107700.*

[5] *Yang, L. (2021) Data Privacy and Recommendation System--Federal Recommendation System. Received from https://www.jiqizhixin.com/articles/2021-07-19-5*

[6] *Tencent Cloud Developer Community. (2023) Data Leakage. Received from https://cloud.tencent.com*

[7] *Zhao, Q. (2024) Generation and Protection of Privacy Legal Issues Under the Background of the Big Data Era. Legal Expo (09), 34-36.*

[8] *Li, J. (2023) Research on APP Privacy Security Issues and Protection Strategies. Network Security Technology and Application (12), 82-83.*

[9] *Xiang, M.M., Jian, L.Y., Li, R., and Guan, X.X. (2024) Latent Class Analysis of Social Media Users' Privacy Concerns from a Cognitive Perspective. Information Science. ISSN 1007-7634.*

[10] *Liu, S.F. (2024) Data Security Risks and Coping Strategies in the Era of Big Data and Artificial Intelligence. Network Security Technology and Application (02), 54-56.*

[11] *Shi, M., and Yang, H.J. (2024) Difficulties and Explorations in Data Privacy Protection for Large Language Models. Big Data Research. ISSN 2096-0271.*

[12] *Meng, X., Hao, W.Q., and Wu, Z.C. (2024) Values, Organizations, and Processes: A Systemic Construction of Privacy Risk Management for Open Data Sharing: Based on Investigations and Implications of British Experience. Information Studies: Theory and Application. ISSN 1000-7490.*

[13] *Yang, Q.Y., Zhang, Y.F., Li, X., and Li, Y.L. (2024) Government Open Data Personal Privacy Protection Policy Guarantee—Content Analysis Based on Policy Practices in Ten Countries. Library and Information Service. ISSN 0252-3116.*