International Journal of Sciences

Research Article Volume 13 – December 2024 (12)

Personal Data Protection in the Current Stage of Internet Marketing: A Research Report

Xiaojing Liu[1]

[1]School of Economics and Management, Qingdao Institute of Technology, Qingdao, 266000, Shandong, China

1 Introduction

1.1 Research Background

In the current digital era, online marketing has emerged as a pivotal strategy for businesses to expand their market reach, augment brand awareness, and drive sales. The rapid advancement of internet technology has facilitated the widespread integration of big data, artificial intelligence, and other cutting-edge technologies in online marketing practices. This integration empowers companies to gather and analyze substantial volumes of user information, enabling precise targeting as a crucial avenue for businesses to promote their products and services effectively. Nonetheless, this process has also engendered grave concerns regarding personal information security. The extensive collection, storage, utilization, and transmission of personal data have introduced significant risks associated with privacy breaches. Once users' personal information is compromised or leaked inadvertently or maliciously by unauthorized entities or individuals, it may result in unwarranted solicitation calls, inundation of spam emails in mailboxes or even severe consequences such as fraudulent activities or identity theft. Consequently, comprehensive exploration into the realm of safeguarding personal information assumes paramount importance amidst this epoch characterized by rapid advancements in online marketing.

1.2 Objectives and Significance

The objective of this study is to acquire a comprehensive comprehension of the current status, prevailing issues, and underlying causes pertaining to personal information protection in network marketing. Correspondingly, countermeasures and recommendations will be proposed. Through this research endeavor, it aims to augment enterprises' awareness and capability in safeguarding personal information during the process of network marketing, thereby fostering the sound development of the industry. Furthermore, it also furnishes a point of reference for relevant regulatory authorities to fortify supervision on personal information protection in network marketing with an aim to ensure users' legitimate rights and interests are duly safeguarded.

2 A comprehensive examination of the theoretical correlation between online marketing and safeguarding personal information

2.1 The Concept and Model of Internet Marketing

Internet marketing is a strategic approach that leverages internet technology and platforms to effectively promote products or services to target users through various sophisticated marketing techniques, including search engine optimization, social media marketing, email marketing, etc. Its primary models encompass content marketing, search engine marketing, social media advertising, email campaigns, mobile advertising strategies, among others. These diverse models differ in their methods and extent of data collection and utilization from individuals.

2.2 The connotation and scope of personal information

Personal information encompasses electronically or otherwise recorded data that, either alone or in combination with other information, can be utilized to uniquely identify an individual. This includes, but is not limited to, the individual's full name, date of birth, identification number, biometric data, residential address, contact number(s), email address(es), health records and travel history. In the realm of online marketing, companies typically gather users' fundamental details along with their consumption patterns and browsing history for analyzing user preferences and behaviors in order to achieve targeted marketing strategies.

2.3 Regulatory frameworks pertaining to the protection of personal information

Both domestically and internationally, a series of laws and regulations have been implemented to safeguard personal information. In China, the Civil Code of the People's Republic of China establishes fundamental provisions for personal information protection. The Cybersecurity Law of the People's Republic of China imposes requirements on network operators regarding the legality, legitimacy, and necessity of collecting and utilizing personal information. Moreover, the Personal Information Protection Law of the People's Republic of China further elucidates rules governing various stages in handling personal information, encompassing collection, storage, use, processing, transmission, provision, and disclosure. These legislative measures

Published at: http://www.ijsciences.com/pub/issue/2024-12/
DOI: 10.18483/ijSci.2810; Online ISSN: 2305-3925; Print ISSN: 2410-4477

Yi Xie (Correspondence)
+86 13811770660

provide a legal foundation and guidance for ensuring personal data security in online marketing.

3 The present state of personal information safeguarding in the realm of online marketing

3.1 Enforcement of laws and regulations

The industry regulatory authorities have also enhanced the oversight of online marketing activities, escalated penalties for illicit and non-compliant behaviors, thereby prompting companies to place greater emphasis on safeguarding personal information.

Since the implementation of laws and regulations such as the Personal Information Protection Law, regulatory authorities have intensified their efforts to combat illegal collection and utilization of personal information in online marketing. Special rectification measures have been implemented in certain regions, imposing penalties on online marketing companies found to have serious personal information security issues. However, due to the intricate nature and extensive reach of the online marketing industry, there still exist numerous challenges in enforcing laws and regulations, including limited regulatory resources and the clandestine nature of illicit activities. Consequently, some companies continue to adopt a risk-taking mentality, leading to occasional violations.

3.2 Measures for enterprise protection

Certain large enterprises have already established comprehensive systems for safeguarding personal information and implemented management protocols, while also reinforcing employee training and education initiatives to heighten awareness regarding the protection of personal data.

3.2.1 Large-scale online marketing enterprise

Certain large-scale online marketing enterprises have established comprehensive systems for safeguarding personal information. For instance, they provide clear notifications to users regarding the purpose, methods, and extent of data collection, proceeding only after obtaining user consent. Encryption technology is employed for secure storage of users' personal information to prevent any potential data breaches. Furthermore, regular security assessments and audits are conducted on their information systems to promptly identify and rectify any security vulnerabilities.

3.2.2 Small and medium-sized online marketing enterprises

Many small and medium-sized internet marketing companies exhibit certain deficiencies in safeguarding personal information. Some companies fail to prioritize the protection of personal data, lacking the necessary expertise and technological capabilities in managing information security. The process of collecting information often involves excessive collection practices, coupled with inadequate security measures that render the collected data vulnerable to potential hacker attacks.

3.3 User awareness and behavior

With the increasing frequency of personal information leakage incidents, users' awareness regarding the protection of personal information is gradually growing. When engaging in online marketing activities, an escalating number of users are becoming mindful of companies' collection and utilization of personal information. Some users opt to withhold their personal information from untrusted entities or meticulously scrutinize relevant privacy policies before providing any data. Users exhibit greater caution when sharing personal information while utilizing online services and express skepticism and dissatisfaction towards unreasonable data collection practices. However, a significant portion of users still possess limited knowledge about safeguarding personal information, which may lead them to overlook their own security when confronted with enticing marketing activities and provide their information to companies without due consideration.

4 Issues of personal information protection in online marketing

4.1 Excessive collection and misuse of information

4.1.1 Overcollecting problems

In pursuit of more precise marketing outcomes, numerous online marketing companies often excessively collect personal information from users that surpasses the necessary requirements for their business operations. This includes gathering users' names, ages, genders, contact details, geographic locations, consumption habits and even unrelated sensitive data. For instance, a basic online shopping platform may demand unnecessary sensitive information like ID numbers and bank card details to complete transactions. Such excessive collection practices heighten the risk of personal data breaches for users. Additionally, some companies neglect to adequately inform users about the purpose, extent and methods employed in collecting their personal information thereby infringing upon their right to be informed.

4.1.2 Information abuse

Some companies fail to adhere to their pre-established commitments and instead exploit users' personal information for alternative commercial purposes, such as selling it to third-party advertisers, resulting in an inundation of unsolicited advertisements. Moreover, internal employees within these companies may also violate regulations and misuse user information, exacerbating the issue of information abuse. The level of personal data protection offered by certain third-party entities varies significantly and can potentially lead to instances of personal information exploitation.

4.2 Vulnerabilities in information security technology

4.2.1 Storage security issues

Certain online marketing companies fail to employ sufficiently robust encryption technology or secure data storage methods when storing users' personal

information, thereby facilitating hackers' easy access to such data by exploiting vulnerabilities in the company's database. Storing personal information poses security risks, including data breaches, cyber attacks, and internal staff misconduct that may result in the unauthorized disclosure of users' personal details. For instance, there have been instances where hackers infiltrated databases of certain companies, leading to the exposure of extensive user information such as names, phone numbers, and addresses.

4.2.2 Transmission security issues

During the process of online marketing, there exist security risks associated with the transmission of users' personal information between enterprises and partners, as well as between enterprises and users. Some companies exhibit inadequate information security management systems and lack effective security measures to ensure the safeguarding of users' personal information. In the absence of secure transmission protocols such as SSL/TLS, unauthorized access or tampering may occur during data transmission.

4.3 Reconciling the tension between personalized recommendations and privacy protection

4.3.1 The principles and privacy implications of personalized recommendations

Personalized recommendation is a crucial aspect of online marketing, employing the analysis of users' browsing history, purchasing behavior, and other personal information to provide tailored product or service recommendations that align with their interests and needs. However, this process necessitates the collection and analysis of extensive user personal data, inevitably raising privacy concerns. Inadequate protection measures during personalized recommendation procedures may compromise user privacy. Consequently, achieving effective personalized recommendations requires substantial access to user personal information while safeguarding their privacy poses a significant challenge.

4.3.2 Reception of personalized recommendations by users

While personalized recommendations offer certain conveniences to users, concerns regarding privacy risks have been expressed by some users. These individuals argue that companies often excessively infringe upon their privacy during the process of conducting personalized recommendations, frequently neglecting to seek full consent or provide sufficient choices when collecting user information for this purpose. Additionally, inadequate consideration of user privacy needs by some companies has resulted in the excessive utilization of personal information.

4.4 Risks in third-party collaborations

4.4.1 The universality of third-party access

In the field of online marketing, companies frequently engage in collaborations with diverse third-party partners such as advertising agencies, data analysis firms, payment platforms, and others. These external entities may potentially access the personal information of users that has been collected by the company during their collaborative business endeavors.

4.4.2 Issues pertaining to the information management of third-party

Due to the varying levels of information security management among third-party partners, failure to conduct rigorous scrutiny and supervision on their information protection capabilities during collaboration may result in the unauthorized disclosure of users' personal information. For instance, certain advertising agents might exploit user data acquired from companies for unrelated advertising campaigns without obtaining proper consent.

5 The analysis of personal information protection issues in online marketing

5.1 The imperfect laws and regulations pose challenges to their enforcement

5.1.1 Loopholes in laws and regulations

Despite the introduction of a comprehensive set of laws and regulations on personal information protection in China, certain aspects still exhibit loopholes. For instance, there is insufficient clarity within relevant legal provisions concerning emerging online marketing models and technological applications, posing challenges for companies to accurately discern the boundaries between legality and illegality in practical implementation. Therefore, it is imperative to further refine and enhance the existing laws and regulations on personal information protection by elucidating specific requirements and standards applicable to online marketing activities while bolstering their operational effectiveness.

5.1.2 Insufficient execution intensity

The enforcement of personal information protection involves multiple departments, leading to coordination challenges. Furthermore, regulatory authorities face limited resources for enforcement and encounter difficulties in promptly and effectively investigating all violations amidst the vast array of online marketing activities. Additionally, the penalties for illegal acts such as personal information leakage may not be sufficiently deterrent in certain circumstances. Therefore, it is imperative to strengthen the promotion and training on laws and regulations pertaining to personal information protection, thereby enhancing legal awareness among enterprises and users.

5.2 Corporate interests and inadequate management

5.2.1 The temptation of economic benefits

By collecting and leveraging users' personal information, companies can achieve precise marketing, enhance marketing efficiency, and boost revenue. However, driven by economic incentives, some companies often overlook the significance of safeguarding personal information and resort to inappropriate practices for data collection and utilization.

5.2.2 Internal management issues in enterprises
Some companies lack a comprehensive personal information protection management system and processes, as well as adequate training on employee information security. Moreover, there is an absence of an effective information security audit and supervision mechanism within the company, impeding timely detection and rectification of employees' violations during the information processing process.

5.3 Insufficient user education and awareness
5.3.1 Insufficient knowledge of user information protection
Many users possess limited knowledge regarding the protection of personal information and remain unaware of which specific data is considered sensitive. Additionally, they lack comprehension of the regulations that companies must adhere to when collecting and utilizing personal information. Consequently, users encounter difficulties in effectively safeguarding their personal information amidst online marketing activities.

5.3.2 Underestimation of privacy risks
Some users often excessively prioritize the convenience and advantages associated with engaging in online marketing activities, while underestimating the potential risks of personal information disclosure. This mindset renders users less vigilant when providing personal information, rendering them vulnerable to information security pitfalls.

6 Suggested measures for enhancing the safeguarding of personal information in online marketing
6.1 Improve laws and regulations and strengthen law enforcement
6.1.1 The refinement and improvement of laws and regulations
Enhance the existing legal regulations on personal information protection by providing explicit guidelines for each stage of personal information collection, utilization, and storage in response to emerging technologies and models in online marketing. For instance, it is crucial to establish comprehensive provisions concerning the safeguarding of personal information during the process of personalized recommendations utilizing artificial intelligence technology. Simultaneously, there should be a clearer definition of illicit behaviors while improving the practicality of laws and regulations. Strengthen public awareness and training programs regarding laws and regulations pertaining to personal information protection to enhance legal consciousness among enterprises and users.

6.1.2 Strengthen law enforcement and supervision
Establish a collaborative law enforcement mechanism among multiple departments, enhance information sharing and coordination between regulatory authorities, intensify enforcement efforts on personal information protection in online marketing, allocate additional law enforcement resources, and impose stringent penalties on violators. Additionally, establish a robust complaint reporting mechanism to encourage users and the public to supervise and report illegal or non-compliant online marketing activities.

6.2 Reinforcing corporate governance and fostering technological advancements
6.2.1 Enhancing the awareness of information protection in enterprises
Enterprises should establish the appropriate business philosophy and consider personal information protection as a pivotal strategy for corporate development. Strengthening employees' information security training and enhancing their awareness of safeguarding personal data will ensure strict adherence to regulations on information protection in their daily work.

6.2.2 Establish and improve information protection systems and procedures
Enterprises should establish a comprehensive personal information protection management system, encompassing standardized processes for the collection, storage, utilization, transmission, and disposal of information. It is crucial to clearly delineate the responsibilities of each department and employee in terms of information protection while establishing an audit and supervision mechanism for ensuring information security. Regular inspections and evaluations should be conducted to assess the company's efforts in safeguarding information.

6.2.3 Reinforce the research, development, and implementation of information security technology
Enhanced investment in research and development of information security technology, incorporating advanced encryption algorithms, access control mechanisms, data anonymization techniques, etc., to bolster enterprises' capacity in safeguarding users' personal information. For instance, employ robust encryption algorithms for securing storage of users' personal data; apply anonymization procedures on sensitive information during user analysis.

6.3 Improve user awareness
6.3.1 Reinforce user education initiatives
The government, enterprises, and social organizations should collaboratively engage in promotional and educational initiatives pertaining to the protection of personal information. Through diverse channels such as online campaigns, community lectures, and school-based education programs, users ought to be educated on the knowledge and skills required for safeguarding personal information. This will empower users to comprehend their rights and responsibilities while acquiring proficiency in identifying and mitigating risks associated with potential breaches of personal data.

6.3.2 Enhancing users' awareness of privacy protection
By promoting education, our objective is to enhance

users' awareness of the risks associated with personal information privacy, thereby fostering a heightened sense of caution when disclosing personal information in online marketing activities. Furthermore, we advocate for active protection of users' legitimate rights and interests upon identification of any infringement upon their personal information.

7 Conclusion

At present, the issue of personal information protection in network marketing is increasingly prominent. It not only concerns the legitimate rights and interests of users but also impacts the sustainable development of the network marketing industry. Through an analysis of the current situation, problems, and reasons for personal information protection in network marketing, it becomes evident that resolving this problem necessitates collaborative efforts from government entities, enterprises, and users. The government should enhance laws and regulations while strengthening law enforcement supervision. Enterprises need to bolster self-discipline and technological innovation. Users must increase their awareness and ability to safeguard their own information. Only through cooperative collaboration among all stakeholders can we effectively protect users' personal information while achieving a healthy development of network marketing with robust personal data protection measures. In future advancements, with continuous technological progressions and growing societal emphasis on personal information security, measures for protecting personal data in network marketing will continue to be refined, fostering a safer online environment for users.

Funding: The present study was supported by Cultivation Project of Qingdao Institute of Technology (Grant No. 2023JY044)