Transactions on Social Science, Education and Humanities Research
ISSN: 2960-1770, eISSN: 2960-2262 | Volume 11
CEPC 2024

Analysis of Personal Privacy Risks and Protection Countermeasures under the Privacy Paradox Dimension

Tingjing Li *

Department of Finance, Zhuhai College of Jilin University, 519040 Zhuhai, China

* Corresponding author: 1807050106@stu.hrbust.edu.cn

Abstract. The privacy paradox is an important issue facing the current digital age, which involves a contradiction between individuals' perceptions of privacy protection and their actual behavior. Despite the general awareness of privacy risks, voluntary disclosure of personal data on digital channels such as social media platforms are still prevalent. This dissertation aims to explore the nature of personal privacy risk under the dimension of privacy paradox and the strategies to deal with it. By analyzing the definition, manifestation and influencing factors of the privacy paradox, combined with the problems and causes brought by personal privacy exposure, this paper proposes protection countermeasures in multiple dimensions, such as legal policies, industry self-regulation, technological means and personal behaviors. With the continuous development and popularization of digital technology, the challenge of personal privacy protection is becoming increasingly severe, but through the comprehensive use of various means and measures, the risks brought about by privacy leakage can be effectively counteracted and personal privacy security can be protected.

Keywords: Privacy paradox; personal privacy protection; digital era; privacy breach.

1. Introduction

In recent years, the proliferation of digital technologies and the advent of the big data era have led to a paradox regarding privacy. The privacy paradox refers to the discrepancy between individuals' expressed concerns about privacy and their actual behavior involving the sharing of personal information online [1]. Although people are generally aware of privacy risks, they are often willing to voluntarily disclose personal data on social media platforms, e-commerce sites, and other digital channels. This contradictory behavior raises significant questions about the nature of privacy in contemporary society and the factors that influence individuals' privacy decisions [2].

Traditionally, privacy security issues are mainly characterized by the conflict between privacy leakage and protection. According to the Statistical Report on the Internet Development Situation in China released by China Internet Network Information Center (CNNIC) in 2023, 68.0% of Internet users said that the Internet is not very secure or very insecure [3]. In addition to incidents such as password theft and consumer fraud, the leakage of various types of sensitive personal information also seriously affects Internet users' sense of online security. Privacy leakage can be categorized into two types: the former is the voluntary dissemination of sensitive information by the subject of privacy, which triggers a privacy security crisis; the latter is the dissemination of information by other people or organizations in possession of private information without the subject's will, resulting in privacy leakage [4].

In the era of traditional media and even web portals, privacy security issues were mainly characterized by the conflict between leakage by others and self-protection. However, with the advent of the era of social network applications characterized by user-generated content, a large amount of personal information is openly shared in cyberspace and stored for long periods, changing the nature of privacy security issues [5]. In the era of social network applications, the self-propagating behavior of privacy subjects introduces new dynamics that intensify the antagonistic conflict between privacy invasion and protection [6, 7].

With the continuous upgrading of the Internet and the popularization of smart devices, the volume and diversity of data generated by people using various applications, especially mobile applications, have increased geometrically, indicating that big data has ubiquitously changed people's daily lives, while at the same time, big data technology has an increasingly serious threat to accurately analyze users' habits, interests, and behaviors [8, 9].

According to the Global Internet User Statistics Report released in 2024, there will be more than 5.3 billion active Internet users worldwide by 2023, representing 65.4% of the global population [10]. By 2025, the number of Internet users is expected to reach 6.54 billion. China has the largest number of Internet users at 1.05 billion, followed by India at 836 million and the United States at 311 million. 92.1% of Internet users primarily use smartphones to browse the Internet. The global reach of social media has increased to 4.74 billion people. The average Internet user spends 6 hours and 40 minutes online each day. 60% of global web traffic comes from cell phone users. Popular communication and social applications, such as WeChat, Facebook, Twitter, Instagram and Jieyin, are moving towards the "3S social concept" of "Show, Share, Discover" [11]. While providing users with more and more convenience, it also increases the risk of privacy leakage. As Bertolucci pointed out, "online privacy concerns have become one of the biggest obstacles to the application and development of big data". In addition to influencing users' online behavior, the benefits gained by users during privacy disclosure also play a crucial role when users engage in online activities When users perceive that the potential risks associated with privacy disclosure outweigh the benefits, they are more likely to choose not to disclose their privacy. Conversely, when users perceive that the benefits outweigh the potential risks, they tend to disclose their privacy. Thus, privacy disclosure behavior of social media platform users often arises from a conflict between privacy concerns and privacy benefits [12].

2. Definition of Concepts

2.1. Definition and Manifestation of The Privacy Paradox

The privacy paradox is a paradoxical situation in which users are concerned about the disclosure of their private information and at the same time are willing to disclose their privacy. This phenomenon originally originated in research in the field of medicine, where a 1998 medical experiment provided a clear case in point [12]. In this experiment, patients resisted the release of clinical material about the medical treatments used on them because they did not want their "privacy" to be publicized. However, when the researchers provided authoritative explanations and supporting evidence, the patients' attitudes changed and they accepted the published clinical materials [13]. This suggests that rational explanations and trust can lead individuals to engage in seemingly irrational behaviors.

The concept of "privacy paradox" first appeared in 2001, and it was not until 2006 that Barmes, an American scholar, found that there was an inconsistency between students' attitudes towards privacy protection and their privacy exposure behaviors through a survey of Facebook student users [14, 15]. This finding puts forward the idea of a "privacy paradox", i.e., users worry that their privacy will be leaked and at risk when using new media, but also generously share personal information on new media platforms, forming contradictory behaviors [16, 17].

2.2. Reasons for the Phenomenon of the Privacy Paradox

In the network era, the way of privacy dissemination has been transformed from the traditional oral and textual transmission to the data code of individuals' behavior on the network [18]. Big data platforms make the dissemination of users' personal privacy on the network faster, deeper and wider by storing, processing and mining the data [19].

With the frequent occurrence of various privacy breaches, users are increasingly concerned about the negative impact of privacy breaches when using social media. Due to the vague concept of "privacy", lack of privacy education or other reasons, users are not able to take appropriate, reasonable and safe ways to deal with security risks when using social media. When users perceive a high risk of privacy

leakage in the process of using social media software, they will exercise stricter control over their privacy management. However, it is difficult for users to accurately and reasonably grasp the degree of privacy management, and if users fail to accurately analyze and assess the privacy risk level, inappropriate privacy exposure behaviors will occur, leading to privacy leakage. The reasons for the phenomenon of privacy paradox are as follows:

In the process of using social platforms, when users feel that the benefits of social media outweigh the risks, they will choose to provide private information according to the usefulness of social media, and what private information to provide depends on how much benefit social media brings to them, the greater the benefit the wider the scope of private data to provide, and vice versa, the smaller the scope of data. The benefits and the scope of privacy data are perceived differently by different users due to different cultural levels and individual perceptions.

Most users know that there is a risk of privacy data leakage in the process of using social platforms, but usually, users overestimate their ability to control the risk underestimate the power of big data platforms and modern technology, and do not pay much attention to the privacy protection instructions when using social media apps. Most users do not read the privacy terms and conditions provided by the platform when using social media apps, or even agree to sign the agreement without reading it, which leads to the contradiction that although users are concerned about privacy leakage and show that they can protect their privacy, they do not reflect it in their actual behavior.

When downloading and using social media apps, most users usually rely on their own experience and immediate needs to judge the security of the apps to immediately use the apps and obtain the corresponding services, thus ignoring the real privacy risks of social media platforms. They even download social media apps from informal channels to fulfil their immediate needs, which further increases the risk of privacy exposure.

Users realize self-presentation by posting personal statuses, comments, uploading avatars, etc. when using social media, which has become one of the main ways for users to actively expose their privacy. There is a lack of specialized personnel control on social platforms, and different users have different standards for judging publicly available information and private information. When using social media, users are more concerned about gaining attention through sharing than about the security of information exposure, which leads to users ignoring privacy and security issues in the socialization process.

Users do not have a good understanding of the various privacy privilege functions of smart devices when they use them, and most of them only discover the functions of smart devices after they start using new devices, and do not pay attention to the collection of sensitive data and the settings of smart devices, which leads to the risk of user information leakage.

3. Problems Posed by the Exposure of Personal Privacy and Their Causes

3.1. Exploration of the Problems Posed by the Exposure of Personal Privacy

The problems posed by the exposure of personal privacy not only hurt individuals, but also have a serious impact on society as a whole. The problems associated with the exposure of personal privacy include the following:

Identity Theft and Fraud: Exposure to personal privacy can lead to identity theft and fraudulent activity, including credit card fraud, fraudulent account opening, etc.

Personal Security Threats: Exposed personal information may be used to track and monitor individuals, resulting in threats to physical safety and property security.

Personal Image Damage: Exposure of undesirable personal information may result in damage to an individual's image and reputation, affecting the individual's standing in society and the workplace.

Pinpointing and tracking: Exposed geolocation information and behavioral data can be misused to pinpoint and track individuals, violating privacy.

Restriction of Personal Freedom: Exposed personal information may be used to restrict an individual's freedom, including internet censorship and physical surveillance.

Targeted advertising and marketing harassment: The use of personal information for targeted advertising and marketing may result in frequent harassment and intrusion of individuals.

Privacy exposure can lead to problems such as identity theft, threats to personal security and image damage, which directly undermine the dignity and rights of individuals. Privacy exposure weakens the foundation of trust in society, and people's distrust of cybersecurity and personal information protection reduces their confidence in society and technology, thus affecting the development of the digital economy and the stability of society. The existence of privacy issues impacts the core values of society, challenges the moral ethical and civilized processes of society, and leads to confusion and instability in social values.

3.2. Analysis of Causes

The deep-rooted causes of the privacy paradox problem involve a variety of factors. Excessive collection and misuse of personal information exist in society, and the continuous development of technology and the drive for commercial interests have also made it easier for personal information to be leaked. Differences in cultural contexts affect individuals' attitudes and behaviors towards privacy protection. Individuals' decisions in the face of privacy exposure are often influenced by psychological factors, such as overconfidence in their security or neglect of the consequences of privacy leakage. Taken together, the solution to the privacy paradox problem requires a comprehensive consideration of social, technological, and cultural factors, and the challenges posed by privacy leakage should be addressed through the formulation of relevant policies and the enhancement of personal information protection awareness.

4. Protection Responses

4.1. Legal Policy Level

Legal policy plays an important role in protecting individual privacy. In March 2023, the Organization for Economic Co-operation and Development (OECD), an intergovernmental organization for international economic cooperation comprising 30 market economies, released a document titled Emerging Privacy-Enhancing Technologies-Current Regulatory and Policy Approaches Report. Privacy Enhancing Technologies (PETs) are usually required by direct or indirect regulations in the privacy and data protection laws and regulations of each country. This is mainly achieved through 1) privacy and data protection law requirements, 2) de-identification requirements, 3) digital security requirements, 4) accountability requirements, and 5) regulatory orders [20].

To complement the above measures, various types of regulatory guidance have been issued by governments or privacy and security-related law enforcement agencies. For example, Article 32 on "Security of Personal Data" of the General Data Protection Regulation issued by the European Union in 2018 provides that "controllers and processors shall take appropriate technical and organizational measures to ensure a level of security appropriate to the risk." The UK's Data Protection and Digital Information Act, published in July 2022, creates a legal test for determining when data will be considered personal or anonymous during data processing. Canada's Treasury Board Secretariat released a Services and Digital Policy in 2020 outlining the need for privacy protection. The policy states that it is the responsibility of the Deputy Minister to "ensure that privacy issues are addressed in the context of any program or strategy that deals with departmental information or data." The above is information on data security requirements, accountability requirements and regulatory requirements. The aim is to ensure the security and protection of personal data and to ensure that organizations comply with relevant data protection laws and regulations. The introduction of laws

and regulations in China, such as the Data Security Law of the People's Republic of China (PRC), which was published on June 10, 2021, and the Law of the People's Republic of China on the Protection of Personal Information (PCPI), which came into effect on November 1, 2021, provide authoritative and mandatory measures for the protection of personal privacy.

These laws and regulations have improved the working mechanism for the protection of personal information by making targeted specifications on the excessive collection of personal information by applications (APPs), preventing big data from killing people, and cracking down on the illegal trading and leaking of personal information. The implementation of these laws and regulations has made it difficult for lawbreakers to find loopholes and gaps to infringe on personal privacy, while also providing victims with a legal basis to protect their legitimate rights and interests. Therefore, continuing to strengthen and improve the laws and regulations on personal information protection, reinforcing law enforcement, and establishing a sound regulatory mechanism will be effective countermeasures to protect personal privacy.

4.2. Industry Self-regulation Level

It is crucial to promote the establishment of privacy protection standards and norms in the relevant industries. The establishment of such standards and norms can help parties in the industry to ensure that personal privacy is adequately protected while promoting the healthy development of the industry. Industry associations and organizations can develop industry standards and guidelines for privacy protection, clearly stipulating norms for the collection, use, storage and sharing of personal information, and ensuring that companies comply with certain rules and requirements when handling personal information. Self-regulatory mechanisms and supervisory bodies can also be established within the industry to oversee and manage the privacy protection behavior of enterprises in the industry and to set up complaint-handling mechanisms to deal with complaints of privacy leakage and infringement promptly, so as to prompt enterprises to strengthen the protection of personal information. Strengthening industry cooperation and exchanges, establishing privacy training and education mechanisms, as well as regularly evaluating and reviewing privacy protection measures are all important initiatives to promote the industry's efforts to establish a sound privacy protection mechanism. Through these efforts, the industry can effectively protect personal privacy, enhance consumer trust in the industry and promote its sustainable development.

4.3. Level of Technical Means

In terms of protecting personal privacy, social software enterprises should pay attention to the security of user information and data and deeply understand the nature of personal information security in the era of big data. To ensure the security of users' personal data, they should take the protection of personal static data security as a starting point and focus on the security of dynamic data in the process of sharing and dissemination of users' personal data under the network environment. By analyzing the risk of data leakage of users' personal information in the process of sharing and dissemination of dynamic data, the establishment of a personal information security protection mechanism that meets the characteristics of the software and the needs of the users, so that the protection of users' personal information security has changed from passive to active. At the same time, social software platforms can carry out hierarchical and sub-authority management of data, and focus on the protection of important data and sensitive data by storing servers to further ensure the security of users' personal data.

The APP's privacy policy should be transparent and complete, clearly stating the way and scope of the social media platform's collection, storage, use and sharing of users' personal information, as well as users' rights and choices. A compliant and reasonable privacy policy can help users rationally analyze the security of social media platforms and make corresponding choices according to their personal needs, thus effectively protecting their personal privacy. In addition, social software companies are able to anticipate users' concerns and avoid the interference of legal issues when formulating privacy policies.

Social software platforms should adopt technical means to increase the difficulty of secondary dissemination of user information. By protecting the personal information that has been posted by users and increasing the difficulty of secondary dissemination of user information, personal information can be effectively prevented from being downloaded, reproduced or saved without authorization. Appropriate measures should be taken, such as obtaining the consent of the author of the original release when the content of the personal display space is downloaded, reproduced, or saved, and notifying and prompting the original publisher promptly after the subsequent act, in order to protect the security of the user's personal information.

4.4. Individual Behavioral Levels

Establishing the right concept of privacy at the individual level. According to the latest data, moderated self-disclosure is one of the keys to effectively controlling privacy leakage. In major online social networking platforms such as WeChat, Facebook, Twitter, Instagram, etc., most of the privacy information leakage is carried out by individuals on their own initiative. Therefore, establishing the concept of moderated self-disclosure, following privacy security guidelines, and clarifying when privacy can and cannot be shared can effectively reduce the frequency of privacy leakage incidents.

Properly open the data collection permissions of smart devices. According to survey data, the search behavior of smart devices is directly related to personal privacy permission settings. When users download and use various social and shopping software, they should carefully analyze the software functions and their own needs, and make restrictive choices for the microphone, address book, camera, gallery, and other permissions of smart devices to reduce the risk of personal information leakage.

Enhance privacy education. According to the latest data, with the advent of the big data era, Internet connectivity has become a necessity of life, and isolation from the Internet is almost impossible. Therefore, it is particularly important to strengthen the awareness of personal privacy and cybersecurity training. Particularly for the youth population, cybersecurity training should be strengthened to raise their level of awareness of online privacy and their ability to control information and to develop their basic ability to recognize the authenticity of information in order to cope with the increasingly complex cyberenvironment and to protect the security of personal privacy.

5. Conclusion

This paper analyzes the risk and protection countermeasures of personal privacy in the dimension of privacy paradox. First, it introduces the concept of privacy paradox and its challenge to personal privacy, and emphasizes the contradictory behaviors of individuals in privacy protection. Subsequently, the problems caused by personal privacy exposure and the reasons for the problems are discussed. On this basis, countermeasures for protection in terms of legal policies, industry self-regulation, technological means and individual behavior are proposed. These countermeasures cover a wide range of levels, from the formulation of laws and regulations to the strengthening of industry self-regulation to the enhancement of personal privacy protection awareness and skills, aiming at comprehensively improving the level of personal privacy protection. In the future, with the continuous development of digital technology, personal privacy protection will face more challenges, and this paper needs to continue to study in-depth the development trend in the field of privacy protection and constantly explore new protection countermeasures to meet the new challenges in privacy protection.

References

[1] Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security, 2017, 64: 122 - 134.

[2] Dienlin T, Trepte S. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European journal of social psychology, 2015, 45 (3): 285 - 297.

[3] China Internet Network Information Center (CNNIC). Statistical Report on the Internet Development Situation in China, 2023.

[4] Young A L, Quan-Haase A. Privacy protection strategies on Facebook: The Internet privacy paradox revisited. Information, Communication & Society, 2013, 16(4): 479 - 500.

[5] Aguirre E, Roggeveen A L, Grewal D, et al. The personalization-privacy paradox: implications for new media. Journal of consumer marketing, 2016, 33 (2): 98 - 110.

[6] Adjerid I, Peer E, Acquisti A. Beyond the Privacy Paradox. MIS quarterly, 2018, 42 (2): 465 - 488.

[7] Hoffmann C P, Lutz C, Ranzini G. Privacy cynicism: A new approach to the privacy paradox. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 2016, 10 (4).

[8] Blank G, Bolsover G, Dubois E. A new privacy paradox: Young people and privacy on social network sites. Prepared for the Annual Meeting of the American Sociological Association. 2014, 17.

[9] Baek Y M. Solving the privacy paradox: A counter-argument experimental approach. Computers in human behavior, 2014, 38: 33 - 42.

[10] We A S. Internet Statistics and Trends, 2024.

[11] Blank G, Bolsover G, Dubois E. A new privacy paradox: Young people and privacy on social network sites. Prepared for the Annual Meeting of the American Sociological Association. 2014, 17.

[12] Bertolucci J. Big data analytics: Descriptive vs. Predictive vs. Prescriptive. Information Week, 2013.

[13] Sun, Baoying, Tang, Jingjing. The Dilemma and Solution of the "Privacy Paradox" in the Mobile Social Era. News Enthusiasts, 2017, 7: 13 - 18.

[14] Sun Qitao. Personalized Service and Potential Harm: A Study of Privacy Consumption in Precision Marketing. Shenyang: Shenyang Normal University, 2021.

[15] Furlong A. Should we, or shouldn't we? Some aspects of the confidentiality of clinical reporting and dossier access. International Journal of Psychoanalysis, 1998, 79: 727 - 740.

[16] Barth S, de Jong M D T, Junger M, et al. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telematics and informatics, 2019, 41: 55 - 69.

[17] Sutanto J, Palme E, Tan C H, et al. Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. MIS quarterly, 2013: 1141 - 1164.

[18] Sun Chaoqun. Research on the Influencing Factors of the Privacy Paradox Phenomenon on Microblog Platform. Dalian: Dalian University of Technology, 2021.

[19] Luo Y., Wei Z., Sun R. Review and Future Prospects of Privacy Paradox Research. Journal of Information Resources Management, 2020, 10 (5): 66 - 75.

[20] OECD. Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches. OECD Digital Economy Papers. 2023.