10.18686/frim.v2i5.4513

# Research on Personal Information Security and Privacy Issues in the Network Environment

**Xiaomei Tang, Xu Gong, Mengqiao Zhang, Peng Zhang, Hailong Li**

**Beijing Union University, Beijing 100101**

***Abstract:*** In today's digital age, we face the grave challenges of personal information security. Frequent hacker attacks, data breaches, social engineering, and illegal information trading pose serious threats to user privacy. By comprehensively applying encryption technology, access control, data desensitization, combined with improved laws and regulations and enhanced user security awareness, these challenges can be effectively addressed, which means, personal privacy can be protected, and a secure and trustworthy network environment can be built.

***Keywords:*** Network Environment; Information Security; Privacy

## 1. Introduction

Rapid development of network technologies has changed our lifestyles, which consequently makes issues concerning personal information security and privacy becoming increasingly severe. From social media to online shopping, our personal information is constantly being collected. Once this information is exploited by criminals, the consequences can be disastrous. Exploring how to protect personal information security and privacy in the network environment has become a crucial issue that society urgently needs to address [1].

## 2. The Current State of Personal Information Security

In today's digital age, personal information security issues are becoming increasingly severe. Hackers frequently attack databases, stealing vast amounts of sensitive data, which is often sold publicly, causing significant distress to users. Many enterprises, due to technical and managerial negligence, frequently experience database vulnerabilities, making them targets for hackers.

Social engineering has also become a common method of information leakage. Through phishing emails and phone scams, criminals can easily obtain users' account information. Illegal trading and commercial misuse of personal information are widespread, with some companies using personal information for advertising and data analysis without user consent. This not only infringes on privacy but also leads to widespread dissatisfaction and concern [2].

The misuse of personal information can even involve identity theft, loan applications, and credit card fraud, causing significant financial losses and psychological stress to victims. More seriously, criminals use this information for criminal activities, threatening personal safety.

## 3. Challenges in Privacy Protection

### 3.1 Manifestations of Privacy Infringement

Privacy infringement in the network environment manifests in various ways. Unauthorized information collection has become a common problem. Many applications and websites quietly collect users' personal data, including location, browsing history, contacts, etc., without their awareness. This unauthorized data collection exposes personal information to unwarranted risks.

Information sharing and exposure are other common forms of privacy infringement. Many companies share collected personal information with third parties, such as advertisers and data analysis companies, without explicit user consent. This information is used for targeted advertising and market analysis, greatly exposing users' privacy. Some social platforms publicly share certain user information to increase social interaction, leading to excessive exposure of user privacy.

Behavioral monitoring is also a significant form of privacy infringement. By tracking users' online behaviors, companies and institutions can gain detailed insights into users' habits, preferences, and interests. This behavioral data is used to provide personalized services but also exceeds user expectations, seriously infringing on personal privacy rights. Every click and search by the user may be recorded and analyzed, making personal privacy impossible to hide.

### 3.2 Difficulties in Privacy Protection

The technical difficulty of privacy protection is a major challenge. Although many advanced encryption technologies and security proto-

cols exist, implementing these technologies requires high costs and expertise. Many SMEs, due to limited resources, cannot effectively protect user data, leading to frequent privacy breaches. As technology advances, hacking methods also continuously upgrade, making data protection more complex and difficult.

The imperfection of laws and regulations is another major difficulty in privacy protection. Although countries actively formulate and improve privacy protection laws, many loopholes remain in actual implementation. Many legal provisions are overly broad, lacking specific operability, and it is difficult to effectively restrain illegal activities. Especially in the context of cross-border data flows, the enforcement of privacy protection laws becomes more complex, increasing regulatory difficulty [3].

Weak user privacy awareness is also a significant challenge. Many users lack basic security awareness while using internet services, casually providing personal information and failing to recognize the importance of privacy settings. Some users even consider privacy protection insignificant, leaving them helpless in the face of privacy infringement and unable to effectively safeguard their rights. Enhancing public awareness and education on how to protect their personal information is one of the pressing issues to be addressed.

# 4. Countermeasures

## 4.1 Technical Measures

In protecting personal privacy and information security, technical measures are undoubtedly one of the most direct and effective methods.

Encryption Technology: Encryption plays a crucial role in ensuring data security. By converting data into an unreadable format, encryption makes it difficult for intercepted data to be illegally read. Modern encryption technologies such as AES (Advanced Encryption Standard) and RSA (Public-Key Encryption) are widely used in various network communications and data storage. Additionally, end-to-end encryption (E2EE) further enhances communication security by ensuring that only the sender and recipient can decrypt and read the information during transmission. This encryption method is widely used in instant messaging applications like WeChat, effectively preventing man-in-the-middle attacks and information leakage [4].

Access Control: Access control is another key technical measure to ensure that only authorized users can access sensitive information. Access control involves various strategies, such as authentication, authorization, and auditing. Authentication verifies the legitimacy of a user's identity through usernames and passwords, biometrics (such as fingerprints and facial recognition), and other methods. Authorization specifies the range of data that users can access and operate, ensuring that sensitive data is only accessible to users with specific permissions. Auditing records all access activities, facilitating the tracking and review of potential security issues. Multi-factor authentication (MFA) is an effective way to enhance access control by combining multiple verification methods, increasing security and reducing the risk of a single authentication method being compromised.

Data Desensitization: Data desensitization protects personal privacy by replacing or masking sensitive information without affecting its actual use. It is commonly used in testing environments and data analysis to ensure that developers and analysts cannot access real sensitive information. Common desensitization methods include pseudonymization and anonymization. Pseudonymization replaces sensitive information with substitute symbols, while anonymization completely removes any personally identifiable information, making it impossible to restore data to individual identities [5]. With the development of big data and artificial intelligence technologies, data desensitization has become increasingly important in ensuring data security and privacy protection while meeting data usage needs.

## 4.2 Legal Regulations

Protecting personal privacy and information security requires not only technical measures but also comprehensive legal regulations.

Development of Privacy Protection Laws: The development of privacy protection laws domestically and internationally provides a legal basis and framework for personal information protection. Internationally, the European Union's General Data Protection Regulation (GDPR) is one of the strictest and most comprehensive privacy protection laws. GDPR sets detailed requirements for how companies handle personal data, including data collection, processing, storage, and transmission, emphasizing the rights of data subjects, such as the right to access, the right to erasure, and the right to data portability. The implementation of GDPR has not only affected companies within the EU but also had a profound impact on global companies [6]. Domestically, China has been continuously improving its legal system for personal information protection. The Personal Information Protection Law (PIPL), passed in 2021, is China's first comprehensive law on personal information protection, marking a significant step forward in personal privacy protection. PIPL stipulates the basic principles and specific requirements that information processors must follow when collecting, storing, and using personal information and clarifies individuals' rights and remedies in information protection.

Case Studies: Typical case studies help us better understand and apply these laws and regulations. For example, in 2018, the UK's Information Commissioner's Office (ICO) fined Facebook heavily for the Cambridge Analytica data breach incident. This incident revealed signifi-

cant privacy risks in how large tech companies handle user data, prompting a substantial increase in global attention and legal enforcement on privacy protection. In China, Didi Chuxing was investigated by the Cyberspace Administration of China for data security issues, reflecting the determination and efforts of domestic regulatory agencies to strengthen data security and privacy protection.

### 4.3 User Behavior

Besides technology and laws, user behavior and awareness play a crucial role in privacy protection.

Raising Security Awareness: Raising security awareness is fundamental for users to protect personal information. Users should understand basic cybersecurity knowledge, avoid entering personal information on untrusted websites, and be cautious with emails and links from unknown sources. Regularly updating passwords and using complex and unique password combinations are effective means to prevent account theft. Users should also be aware of common social engineering attacks, such as phishing emails and fraudulent calls, enhancing their prevention awareness to avoid being exploited by criminals.

Optimizing Privacy Settings: Optimizing privacy settings is a key step for users to actively protect personal privacy. When using various applications and services, users should carefully read privacy policies to understand how their data is used and shared. Minimizing the amount of publicly shared personal information and carefully setting privacy permissions on social platforms ensure that only trusted friends can see their updates and information. Disabling unnecessary location sharing and restricting application permissions are also important measures to protect personal privacy. Many platforms provide detailed privacy setting options, and users should make good use of them, regularly checking and adjusting these settings to meet their privacy needs.

## 5. Conclusion

Protecting personal privacy requires the joint efforts of the whole society. Through the comprehensive measures of technology, laws, and user behavior, we can effectively address the challenges of privacy protection and ensure that personal information receives the security it deserves in the digital age. Only by working together can we achieve true network security and privacy protection.

## References

[1] Yan Xianglin. Analysis of personal information security and privacy in the network environment [J]. information science, 2002, 20(9):937-940.

[2] Yang Xiaowu, Xie Shunjun. Research on the legal protection of personal information under the network environment [J]. Chutian rule of law, (23):0034-0036.

[3] Wang Yuwei. Research on personal information protection under the background of the Internet[J]. 通讯世界, 2024, 31(3):45-47.

[4] Chao Lu. Research on the security of computer personal information in the network environment [J]. Computer knowledge and technology2016, 12(10):29-30+35.

[5] Al-Charchafchi A, Manickam S, Alqattan Z N M. Threats against information privacy and security in social networks: A review[C]// Advances in Cyber Security: First International Conference, ACeS 2019, Penang, Malaysia, July 30–August 1, 2019, Revised Selected Papers 1. Springer Singapore, 2020: 358-372.

[6] Rahman H U, Rehman A U, Nazir S, et al. Privacy and security—limits of personal information to minimize loss of privacy[C]//Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC), Volume 2. Springer International Publishing, 2020: 964-974.