Assessing the Impact of Implementing Social Media Privacy Laws: Analyzing Data Based on User Behavior

Jinqi Li

The London School of Economics and Political Science, London, United Kingdom

J.Li261@lse.ac.uk

Keywords: Social media; Privacy protection; Enforcement of laws; User behavior; Data analysis

Abstract: In the digital age, social media has undoubtedly become an important platform for communication and sharing their personal lives. As user interactions and information exchanges become more frequent, it is crucial for the public to recognize the importance of data protection and disclosure on social media platforms. Therefore, social media privacy laws emerged to balance the trade-off between public safety and personal privacy. This paper examines user behavior data and evaluates the effectiveness of current privacy protection laws. The goal is to reveal the impact of legal provisions on user privacy protection and to provide insights for future legislation and policy adjustments. The widespread use of social media has given birth to many laws and regulations on privacy protection. To effectively evaluate the implementation effect of the legal policies, a comprehensive analysis of the behavior data of social media users is necessary. This study collected user data from many social platforms and analyzed users' behavior patterns on social media using data mining technology. Additionally, it focused on observing changes in user behavior before and after implementing privacy protection laws. The research indicated that after implementing the laws, users demonstrated more cautious behavior regarding data protection. It included being more careful about information sharing, managing their friend lists, and adjusting their account settings. These findings suggest that the relevant legal policies positively impact the public.

1. Introduction

With the rapid development of globalization, social media has become an indispensable part of people's daily lives. Users can stay connected with family and friends on various platforms, quickly obtain information, and engage in global conversations [1]. However, the popularity of social media has also brought a series of issues related to privacy security, which affect individuals' information security and mental health. To address these challenges, countries have enacted a series of laws for data protection, aiming at protecting users' personal information from infringement.

Despite these laws, privacy issues on social media are still frequent, which has aroused widespread concern among the public and scholars. Assessing the implementation effects of these laws will enable researchers to evaluate the effectiveness of current laws and policies, providing a foundation for their improvement and enhancement. Therefore, based on user behavior data, this study will systematically analyze the results of implementing social media privacy laws through quantitative and qualitative methods. Moreover, this paper will discuss the influence of law enforcement on the behavior patterns of ordinary users and how these laws shape users' cognition and attitudes toward privacy.

2. Theoretical Basis and Framework

2.1 The Basic Principles and Objectives of Privacy Protection Law

Privacy protection laws are formulated and implemented to safeguard personal information from excessive collection, use, disclosure, or destruction. Internationally, the *General Data Protection Regulation* (GDPR) is the most famous one, and it provides a widely imitated template for privacy protection legislation [2]. Privacy protection laws are usually based on the following principles:

  DOI: 10.25236/gemmsd.2025.028

Lawfulness, fairness, and transparency; purpose limitation and data minimization; Accuracy and storage limitations; Integrity and confidentiality; and accountability. These principles create a protective framework to safeguard users' data.

The law is published to realize the autonomy of personal information, reduce the invasion of privacy, enhance the public's understanding and respect for the right to privacy, and encourage enterprises and institutions to establish privacy protection policies with higher standards. By showing liability limits for data controllers and processors, requesting access to individuals, and modifying or destroying them. If necessary, the personnel have access to take appropriate actions to fight against illegal acts. In summary, the law aims to create a digital social environment that attributes privacy to the public and respects all privacy.

2.2 The Theoretical Framework of User Behavior Analysis

User behavior analysis involves a series of quantitative and qualitative research methods to identify and explain people's behaviors and patterns in a specific environment. On social media, user behavior covers a wide range of content, such as content publishing frequency, content types, and interactive forms. Data can be obtained through the social media platform's API interface and analyzed through statistics, machine learning, and natural language processing [3].

The theoretical framework is constructed using three dimensions: psychological motivation, method, and behavioral influence. Its purpose is to identify and analyze the behavior patterns of users driven by specific motives and evaluate how these behaviors change when influenced by external factors, such as law enforcement. By examining personal information management habits from a psychological and behavioral perspective, this framework allows us to speculate on the social behavior trends that may arise from legal changes.

2.3 The Theoretical Model of the Relationship between Privacy Protection Law and User Behavior

We can use a theoretical model to systematically explain the relationship between privacy protection law and user behavior. The model regards users' privacy behavior as a function of their awareness of privacy laws, risk perception, interest evaluation, and personal privacy characteristics. Enforcing the law will enhance users' understanding and decrease their risk perception, thereby encouraging more proactive privacy protection [4].

The model examines the direct and indirect effects of laws on users' behavior, including the impact of users' right to know and participate, legal compliance, and social belonging on their privacy behavior. The theoretical model points out that based on legal dissemination and widespread recognition, individuals' sense of self-efficacy in privacy protection is improved. The conclusion is that it helps to form a more active strategy for protecting data privacy. In addition, the model considers the influence of social, cultural, and technical factors. Different environmental factors may have complex mechanisms for privacy protection. Empirical research can effectively evaluate the implementation of privacy protection laws.

3. Implementation Status of Social Media Privacy Laws

3.1 From the International Perspective: An Overview of Privacy Protection Laws

Many countries in the international community have enacted various laws and regulations to protect data privacy. The *General Data Protection Regulation* (GDPR) in Europe is one of the most significant examples of data protection legislation. Since it entered into force in 2018, GDPR has profoundly impacted how enterprises handle personal data. According to the GDPR, any organization that processes EU citizens' data must adhere to stringent protection principles [5]. Enterprises that violate these regulations may incur substantial financial penalties. For example, in 2019, British Airways was fined 1.83 million pounds by the British Information Commission for data leakage in 2018, reflecting the strict implementation of GDPR legal provisions.

It is also worth mentioning that the *California Consumer Privacy Act* (CCPA) in California,

which was enacted in 2020, gives consumers the right to know, refuse to sell personal information, and access and delete personal information. At the beginning of implementation, many technology companies, such as Facebook and Google, quickly adjusted their privacy policies to comply with the new regulations. In addition, the California legislature passed the *California Privacy Rights Act* (CPRA), which took effect in 2023, strengthening CCPA and providing stricter data protection.

3.2 From the Domestic Perspective: The Implementation of Social Media Privacy Laws in China

In China, due to the rapid development of the Internet, social media platforms such as WeChat and Weibo are playing an increasingly important role. The Chinese government has increasingly focused on protecting online privacy by implementing various laws and regulations to enhance user privacy protections [6]. For example, in 2017, China promulgated the *Cyber Security Law*, the basic law to ensure cyber security and maintain the rule of law in cyberspace.

In a real case, with the help of *Cyber Security Law*, Chinese supervisors in 2018 looked into improper handling of user data in an incident in which a driver killed a passenger with a Didi Taxi and released a rectification notice. The *Civil Code* enacted in 2020 enhanced the protection of personal information and clarified the principles of legality and rationality to be followed in handling such information.

Furthermore, China has recently promulgated the *Data Security Law* and *the Personal Information Protection Law of the People's Republic of China*. The law's enactment signifies a new phase of data privacy protection in China. The *Personal Information Protection Law* emphasizes user consent and imposes significant fines for violations.

3.3 Comparison and Difference Analysis of Laws and Regulations

We can observe significant differences in structure and focus when examining the social media privacy laws in various countries. Europe's GDPR highlights rules for handling cross-border data and high fines for companies that break the rules, and its influence extends to companies outside the EU. In contrast, CCPA and CPRA laws in the United States are more inclined to enhance consumer control, and there is currently no unified national privacy protection legislation.

China's *Network Security Law* and *Personal Information Protection Law* focus more on national security and social public order. Additionally, the law is progressively enhancing the rights of data subjects. These variations reflect different countries' diverse social cultures, political systems, and legislative concepts.

The analysis of specific cases demonstrates that although the fundamental principles of legislation are similar, cultural differences and varying enforcement efforts result in privacy protection laws being implemented differently across countries. For instance, U.S. technology companies have updated their privacy policies due to legislation in California, while companies in China may shape their privacy protection practices more through national policies.

4. Case Analysis

4.1 Case Selection Criteria and Basis

In evaluating the implementation effect of social media privacy laws, it is vital to select representative cases. First, the case should involve diverse user groups and demonstrate significant social impact to ensure that it has attracted substantial public attention and sufficient data to support the analysis. Second, the case should involve internationally renowned social media platforms, as their policies and practices often set industry standards. Finally, it is suggested that the case be accompanied by a definitive legal response and subsequent social and user behavior responses, which would be to evaluate the actual effect of legal measures.

According to the criteria mentioned above, this paper chooses Facebook users' privacy disclosure as the object of analysis in international cases. Following the incident, a global discussion on data privacy protection emerged, prompting Facebook and regulators to implement substantial measures.

This case offers valuable insights into the relationship between privacy protection laws and user behavior [7].

4.2 International Case: Facebook's Privacy Leak and Legal Responses

4.2.1 A Review of Events

In 2018, the scandal of Facebook users' privacy disclosure broke out, and it was found that Cambridge Analytica, a third-party company, was allowed to collect the personal data of about 87 million users through a psychological test application. This incident shocked the international community as it involved leaked personal data and online behavior used for political advertising targeting.

4.2.2 Legal Measures

After the incident, Facebook suffered from strong pressure from governments worldwide. In Europe, regulators quickly launched an investigation into Facebook, demonstrating the strict regulatory approach mandated by the GDPR. The US Federal Trade Commission (FTC) also launched an investigation into Facebook. It reached a historic $5 billion settlement agreement with Facebook in 2019, stipulating that Facebook must take stricter privacy protection measures.

4.2.3 Analysis of User Behavior Changes

After the Facebook users' privacy disclosure, many users began re-evaluating their privacy settings on social media. According to the research, a significant number of users changed their privacy settings after the incident, which restricted the access rights of apps. The incident led to significant changes in social behavior, making people more cautious about sharing personal information. Additionally, it sparked public discussions about the importance of privacy. Many users began advocating for more transparent data processing policies and called for stricter regulation of social media companies.

Despite these changes, the overall user activity has not experienced a significant decline in the long term. While privacy leaks have heightened users' concerns about privacy protection, the significance of social media in contemporary life prompts many users to continue engaging with these platforms. Additionally, it implies an interesting phenomenon: a certain degree of trade-off between users' concern for personal privacy and their dependence on social media.

4.3 Domestic Case: Weibo's Privacy Protection Policy Adjustment and User Response

4.3.1 Policy Adjustments

Weibo, one of China's largest social media platforms, has attracted a lot of attention due to the adjustment of its privacy protection policy. In recent years, Weibo has adjusted its data protection policies to promote national laws and regulations and enhance public privacy awareness. For example, protecting personal information introduces a clearer user consent mechanism and strengthens user data's encrypted storage and transmission. There are also stricter measures for the supervision of third-party application access platforms, requiring these apps to inform users of the purpose, scope, and methods of data collection.

4.3.2 User Feedback and Behavior Changes

Users' feedback shows a polarized trend for the adjustment of Weibo's privacy policy. Some users articulated their appreciation for enhanced privacy protection, attributing their heightened trust in the platform and increased propensity to share personal information to this feature. On the other hand, some users have reservations about the policy adjustments. There are concerns that its effective implementation may be questionable despite the policy seeming strict. Updating the privacy policy encourages users to take greater responsibility for managing their personal information. Some users started to organize the list of concerns and limit the visible range of accounts to decrease the risk of personal information exposure. There are some blog posts and discussions on the platform to educate users on how to better protect their private data, which

reflects the improvement of privacy protection awareness.

4.3.3 Effectiveness and Deficiencies

The policy adjustment has achieved initial results in raising users' awareness of privacy protection and promoting the public to discuss their rights to privacy. However, challenges also exist. At the executive level, it is extremely difficult to fully supervise and protect the privacy of all users because of the huge user groups and diverse behaviors on Weibo. Although the policy has been adjusted, information leakage and privacy violations have occurred occasionally. For instance, the user comments associated with certain high-profile events may not fully prevent the unauthorized disclosure and dissemination of information, thereby creating a vulnerability in user privacy protection.

Furthermore, the imbalance in users' awareness of privacy protection is a challenge for the platform manager. Many users are confused about the complexity of privacy settings and do not fully use the privacy protection tools provided by Weibo. The phenomenon is particularly evident among new users and elderly users. Therefore, education to improve users' privacy protection skills is particularly important in addition to policy adjustment.

To sum up, the changes in Weibo's privacy protection policy indicate progress in data privacy protection in China, though there remains room for improvement in how it is implemented and in user education. By implementing the *Personal Information Protection Law* and other regulations, Weibo is expected to adopt more effective measures to safeguard users' rights.

5. Conclusion

Social media privacy laws are becoming a global issue, and countries have adopted legislation to strengthen the supervision of social media platforms. For example, GDPR in Europe and the *Personal Information Protection Law* in China all show attention and efforts to protect personal privacy under different cultural backgrounds and requirements. However, the differences are reflected in the specific contents, enforcement of legal provisions, and the emphasis on users' privacy rights among countries.

Social media companies in many countries and regions have adjusted and perfected their policies because of legal pressure and public opinion. For example, the changes made by Facebook to its privacy policy and the following adjustments by Weibo illustrate the mutual influence between corporate policies and legal regulations. Good privacy protection measures enhance users' trust in the platform, and the shortcomings need to be addressed by legal and administrative means.

Despite adjusting laws and policies, user behavior and privacy awareness improvements are gradually evolving. Although users generally put higher requirements for privacy protection, they still show inconsistency between cognition and action in their behavior. The significance of social media in contemporary life leads users to balance privacy concerns and their reliance on social networks.

In conclusion, researchers need to comprehensively use policies, technologies, and education to improve the implementation effect of social media privacy laws. Regulators need to constantly update the response mechanism to technological advancement to prevent new challenges to privacy protection. Enterprises must strengthen the transparency and user-friendliness of privacy protection measures and provide more intuitive privacy settings. Additionally, creating privacy and enhancing personal data protection is key to improving overall data protection for the public.

References

[1] Aichner T, Grünfelder M, Maurer O, et al. Twenty-five years of social media: a review of social media applications and definitions from 1994 to 2019[J]. Cyberpsychology, behavior, and social networking, 2021, 24(4): 215-222.

[2] Andrew J, Baker M. The general data protection regulation in the age of surveillance capitalism[J]. Journal of Business Ethics, 2021, 168: 565-578.

[3] Huang C. A meta-analysis of the problematic social media use and mental health[J]. International Journal of Social Psychiatry, 2022, 68(1): 12-33.

[4] Erforth B, Martin-Shields C. Where privacy meets politics: EU–Kenya cooperation in data protection[M]//Africa–Europe Cooperation and Digital Transformation. Routledge, 2022: 142-155.

[5] Johnson G A. Economic research on privacy regulation: Lessons from the GDPR and beyond[M/D/C]//Goldfarb A, Tucker C E (eds). The Economics of Privacy. Chicago: University of Chicago Press, 2024: 97-126. DOI: 10.7208/chicago/9780226834085.003.0005.

[6] Allahrakha N. Balancing cyber-security and privacy: legal and ethical considerations in the digital age[J]. Legal Issues in the digital Age, 2023 (2): 78-121.

[7] Hasal M, Nowaková J, Ahmed Saghair K, et al. Chatbots: Security, privacy, data protection, and social aspects[J]. Concurrency and Computation: Practice and Experience, 2021, 33(19): e6426.