GEORGE BROWN PRESS
JOURNALS, BOOKS & PROCEEDINGS

*GBP Proceedings Series*

*Article*

*2024 International Conference on Art and Design, Education, Media and Social Sciences (DEMSS 2024)*

# Study on Countermeasures for the Protection of Consumers' Personal Information Rights from the Perspective of Civil and Commercial Law

**Zhouyang Shen** [1,*]

[1] Kenneth Wang School of Law, Soochow University, Suzhou, 215006, Jiangsu, China
* Correspondence: Zhouyang Shen, Kenneth Wang School of Law, Soochow University, Suzhou, 215006, Jiangsu, China

**Abstract:** With the advent of the information age, data has become a new factor of production, and the collection, storage, and utilization of consumers' personal information have become increasingly frequent. However, while these technological advancements bring convenience to society, they have also triggered numerous issues related to privacy leakage and data misuse, severely eroding consumers' rights to personal information. From the perspective of civil and commercial law, this paper aims to delve into the current state, problems, and countermeasures of protecting consumers' personal information rights. It seeks to uncover the shortcomings of the existing legal system in addressing the challenges of data protection. By proposing systemic legislation, diversified regulatory mechanisms, enhanced corporate responsibilities, and heightened consumer awareness, among other multi-dimensional measures, a more robust framework for protecting consumers' personal information is envisioned, with the hope of providing valuable references for future judicial practices.

**Keywords:** consumers' right to personal information; civil and commercial law; data protection; privacy breaches

Received: 02 December 2024
Revised: 09 December 2024
Accepted: 26 December 2024
Published: 04 January 2025



## 1. Introduction

With the rapid advancement of information technology, the significance of data in contemporary society has become increasingly prominent, serving as a crucial driving force propelling economic development and societal progress. Consumer personal information, as an integral component of data, not only pertains to individual privacy and dignity but also directly impacts personal property interests and social rights. However, amid the convenience brought by the information age, incidents of personal information rights being violated occur with regularity; they range from being exploited for commercial marketing to causing significant financial losses and even posing risks to personal safety. The frequent occurrence of these issues not only reveals the inadequacies in the legal framework but also underscores the contradictions between technology and ethics. Consequently, it is imperative to re-examine the protection of consumer personal information rights from the perspective of civil and commercial law, exploring issues such as legal institutions, administrative supervision, corporate responsibilities, and consumer duties.

## 2. Theoretical Basis for the Protection of Consumers' Right to Personal Information

### *2.1. Definition of the Concept of Consumers' Right to Personal Information*

The right to personal data of consumers is not merely a straightforward entitlement; it involves multi-faceted protections encompassing personal privacy, dignity, and property interests. Broadly speaking, the right to consumer personal information refers to the consumers' authority to control and utilize their personal data, a right that encompasses various aspects including the collection, use, storage, transmission, and processing of personal data. However, in practical applications, this concept often faces ambiguities and ill-defined boundaries, such as what constitutes personal information and when collection becomes lawful—key issues that require in-depth exploration. Existing laws vary significantly in defining personal information, with differing expressions across various legal documents, leading to potential conflicts and gaps in actual protection. With the advancement of new technologies, the scope of personal information is constantly expanding, including novel types such as biometric and geolocation data, for which the legal protections are notably inadequate. This not only affects consumers' rights but also poses significant challenges to corporate compliance. Therefore, clearly delineating the definition and scope of consumer personal information is crucial for formulating effective protection measures. Properly defining personal information can enhance the transparency and operability of the law, while also better balancing the rights of consumers and the interests of enterprises [1].

### *2.2. Legal Attributes of Consumers' Right to Personal Information from the Perspective of Civil and Commercial Law*

From a civil and commercial law perspective, the legal nature of consumers' personal information rights has long been a hot topic of discussion in the academic and legal communities. Some argue that personal information rights should be categorized under the realm of personality rights, emphasizing the close correlation between personal information and individual dignity and privacy. Protecting personal information is thus seen as a means to safeguard the integrity and freedom of the individual's personality. Conversely, another viewpoint posits that these rights belong to the domain of property rights, as personal information holds economic value and can generate material benefits for the individual. Yet another perspective considers personal information rights to be a composite right, incorporating both personality and property attributes, which better aligns with the realities of modern society. Information not only pertains to individual privacy and dignity but also intersects with economic interests and social rights. Given this composite nature, safeguarding consumers' personal information rights necessitates a balanced consideration of various interests. In legislative and judicial practices, it is imperative not to emphasize personality rights or property rights exclusively but to seek harmony between the two. For instance, in commercial activities, the exploitation of personal information should be strictly regulated to ensure that individual privacy is not violated; conversely, in cases involving public interest, the use of personal information may require more flexibility. The legal framework should effectively address a myriad of complex scenarios, balancing the protection of personal privacy with the advancement of social and economic development. Such a framework not only lends itself to greater legal persuasiveness but also better upholds consumers' rights in practical applications.

## 3. Problems in the Protection of Consumers' Right to Personal Information from the Perspective of Civil and Commercial Law

### *3.1. Legal System Level*

Despite the recent enactment of relevant laws and regulations, significant shortcomings persist. On one hand, the current legal framework lacks clarity in defining and delineating the scope of personal information, making it difficult to ascertain which specific data qualifies as personal information and which information's collection and utilization

should be subject to stringent regulation. This ambiguity not only complicates law enforcement but also enables some enterprises to exploit loopholes, using various pretexts to abuse consumer personal data. On the other hand, existing laws and regulations exhibit limitations in their protective measures and coverage. For instance, while the Consumer Rights Protection Law includes provisions on personal information protection, these are relatively simplistic and lack concrete, actionable guidelines. Though the Cybersecurity Law and the Personal Information Protection Law have somewhat mitigated these deficiencies, there remain legal voids in certain specific areas such as biometric and healthcare information. This renders the law's lag and imperfection more evident when dealing with new technologies and applications. Additionally, existing laws and regulations are also weak in their delineation of legal liabilities. The penalties prescribed for infringing upon consumers' personal information rights are insufficient to deter effectively, leading some enterprises to gamble on flouting the law in the face of substantial economic incentives. Furthermore, the coordination and consistency between various legal statutes need to be strengthened. For example, there are conflicts in regulations concerning cross-border data transfer and data sharing across different legal documents, causing confusion for enterprises in their compliance efforts and leaving consumers' rights inadequately protected. These issues not only undermine the practical effectiveness of the law but also leave consumers feeling helpless and disillusioned when their personal information is infringed upon. Therefore, it is essential to establish a more comprehensive legal system, which would clarify the definition and scope of personal information and enhance the enforcement of legal liabilities [2].

### *3.2. Administrative Supervision Level*

In contemporary times, despite the multitude of measures implemented by various levels of government and regulatory bodies, the persistent infringement of personal information continues unabated, primarily due to the limitations of regulatory resources and the lagging technological means. For instance, when faced with the vast and intricate activities involving the use and processing of personal information, regulatory authorities often struggle to exert comprehensive and effective oversight, thereby enabling some enterprises to operate in a gray area where consumer information security is significantly jeopardized. Moreover, the unclear delineation of responsibilities among different regulatory bodies leads to frequent cases of buck-passing and bureaucratic tangling during actual supervision, further exacerbating the lack of coordination and unity within the regulatory framework. This fragmented oversight mechanism results in many issues remaining unresolved in a timely and effective manner. Additionally, the existing administrative penalties are relatively mild, often failing to constitute a substantial deterrent for enterprises. Driven by economic interests, some companies are willing to bear the cost of fines and continue their practices of infringing upon personal information, thereby not only undermining consumer rights but also eroding public trust in regulatory institutions. Furthermore, the transparency of administrative supervision and the level of public participation are insufficient. For example, in decision-making processes concerning personal information protection, public opinions and suggestions are frequently overlooked, causing regulatory policies to lack a foundation of public will and social support. This state of affairs leaves consumers feeling unheard and exacerbates their concerns about personal information security. Simultaneously, regulatory bodies often appear ill-equipped when dealing with new technologies and emerging application scenarios. With the advent of big data and artificial intelligence, the collection and utilization of personal information have become more covert and complex, rendering traditional regulatory methods inadequate and thereby increasing the risks to consumers' personal information. In summary, the issues at the administrative regulatory level not only hinder the practical effectiveness of personal information protection but also leave consumers feeling helpless and disillusioned when faced with infringements.

### *3.3. Enterprise Level*

On the corporate level, the issue of protecting consumers' rights to their personal information is also quite pronounced. Many enterprises, in their pursuit of commercial interests, overlook the protection of consumers' personal information, leading to frequent occurrences of data breaches and misuse. On one hand, businesses often collect personal information in overly broad scopes and at excessively frequent intervals, failing to fully consider the actual needs and privacy protection concerns of consumers. Such excessive data collection not only increases the risk of information leakage but also leaves consumers feeling disquieted and violated. On the other hand, businesses often lack transparency in handling personal information. Many consumers are unaware that their data is being used for third-party marketing, data analysis, and other purposes. In these opaque operations, businesses frequently reap significant benefits while neglecting consumers' fundamental rights to be informed and to choose. This imbalance in information control makes it difficult for consumers to effectively protect their rights when their personal information is misused. Additionally, there are deficiencies in how enterprises establish mechanisms for protecting personal information. Many enterprises have inadequate internal management and technical safeguards, making personal information vulnerable to hacking or internal breaches during storage and transmission. Some companies even view personal information protection as a dispensable add-on, unwilling to invest sufficient resources and effort to enhance related protective measures. This attitude not only reflects a lack of corporate responsibility but also intensifies the security risks associated with personal information. Furthermore, businesses frequently impose unfavorable terms on consumers through standardized contracts. These include "one-size-fits-all" authorization clauses in privacy policies, compelling consumers to relinquish considerable control over their personal information when using services [3]. Such unreasonable terms impose a significant cost on consumers' privacy, even as they enjoy the convenience of the services. This short-sighted behavior not only harms consumers' interests but also impacts the long-term development and social image of the enterprise. Therefore, enterprises should place greater emphasis on personal information protection, not merely to comply with laws and regulations, but also to gain consumers' trust and support.

## 4. Countermeasures and Suggestions for Strengthening the Protection of Consumers' Personal Information Rights under the Perspective of Civil and Commercial Law

### *4.1. Improve Relevant Legislation and Build a Systematic Legal System*

In the current legal framework, the definition and scope of personal information require further clarification to reduce ambiguity and provide clearer legal guidance in practical operations. For instance, sensitive information such as biometric data and medical health information within specialized domains could be incorporated into the legal protection regime to ensure their comprehensive safeguarding. Additionally, legislative efforts should focus more on the establishment of concrete, actionable provisions. For example, the Consumer Rights Protection Law could be augmented with detailed stipulations on personal information protection, clearly delineating the specific obligations and responsibilities of enterprises in the collection, use, storage, and transmission of personal information. This would more effectively constrain corporate behavior and mitigate instances of infringement. Moreover, the legal framework should strengthen the regulations concerning administrative penalties, increasing the cost of illegal activities. For instance, more stringent fines could be established, and even criminal penalties introduced, to deter potential infringers. Furthermore, the law should encourage and support consumer litigation by establishing specialized channels for complaints regarding personal information protection and streamlining the litigation procedures. For example, dedicated personal information protection units could be set up within all levels of consumer associations to provide professional consultations and assistance, ensuring that consumers re-

ceive timely and effective support when faced with infringement of their personal information. A robust legal system governing the cross-border transfer of personal information should also be established, clarifying the responsibilities and obligations of enterprises in cross-border data transfers and mitigating risks associated with the international circulation of personal information. In summary, constructing a comprehensive, systematic, and actionable legal framework not only provides robust protection for consumer rights but also serves as a reasonable standard for corporate behavior, fostering a healthy and orderly market environment in the digital age. This environment would enable consumers to use various digital services with greater confidence, while enterprises, operating within the bounds of legality and compliance, could develop and thrive more effectively [4].

### *4.2. Strengthen Administrative Supervision and Build a Diversified Supervision Mechanism*

Currently, frequent incidents of personal information leakage are significantly related to insufficient administrative regulatory oversight. In the pursuit of profit, enterprises occasionally overlook laws and regulations pertaining to personal information protection. To effectively deter such violations, it is imperative for regulatory authorities to intensify both inspections and penalties. For instance, a cross-departmental joint regulatory task force could be established, involving multiple agencies such as the Ministry of Industry and Information Technology, the Cyberspace Administration, and the State Administration for Market Regulation. These agencies would convene periodically to analyze emerging issues and challenges in personal information protection, coordinating their regulatory actions. Furthermore, regulators should increase technological investment to enhance their supervisory capabilities. For example, specialized monitoring platforms could be developed, leveraging big data and artificial intelligence technologies to continuously monitor enterprises' data processing activities, swiftly identifying suspicious behavior. A robust reporting and complaint mechanism is also essential. Official websites and mobile applications of departments such as the Industry and Commerce Bureau and the Market Supervision Administration should feature convenient reporting channels, encouraging consumers and the public to actively participate in oversight. Rewards could be offered to informants to motivate broader participation. Regulatory bodies should conduct regular inspections of enterprises to ensure compliance with personal information protection laws and regulations. For example, unannounced surprise inspections could be conducted to scrutinize potential violations, with immediate corrective actions demanded for non-compliant firms. Severely violating enterprises must be strictly sanctioned according to the law, making them bear the due consequences. This would underscore to them that the cost of infringing upon personal information is substantial, far surpassing any short-term benefits they might gain. Additionally, regulators should strengthen international cooperation to jointly address cross-border data breaches and infringements. For instance, information sharing mechanisms could be established with international data protection agencies to promptly obtain risk information related to cross-border data transfers, facilitating coordinated efforts against transnational crimes. By implementing these measures, a comprehensive and efficient regulatory network can be formed, ensuring robust protection of consumers' personal information. This not only safeguards consumer rights but also standardizes market order, fostering the healthy development of the digital economy.

### *4.3. Strengthen Corporate Responsibility and Build a Data Security Guarantee System*

In the information age, businesses play a pivotal role; however, many enterprises, in their pursuit of profit maximization, often neglect the paramount importance of data security. This short-sighted approach not only undermines the rights and interests of consumers but also jeopardizes the long-term development and social image of businesses. Therefore, enterprises must take concrete steps to strengthen their data security safe-

guards. Firstly, businesses should establish robust internal data security management systems, clearly delineating the responsibilities and obligations of various departments and employees in data protection. For instance, the creation of dedicated data protection officers or departments can oversee and supervise data security efforts, ensuring that every aspect is meticulously managed and that any vulnerabilities are promptly identified and addressed. Secondly, enterprises should augment their technical investments to enhance data protection capabilities. Advanced encryption techniques and security measures should be implemented to ensure data security during the collection, transmission, and storage processes. Introducing multi-factor authentication mechanisms and dynamic encryption technologies, for instance, can significantly mitigate the risks of unauthorized data access. Furthermore, businesses should conduct regular data security training for their employees to elevate their awareness and skills in data protection. This not only helps employees better understand legal and regulatory requirements but also enhances their ability to prevent data breaches in their daily operations. Additionally, enterprises should develop comprehensive data security emergency response plans to swiftly mitigate losses and impacts in the event of a data breach. Establishing specialized emergency response teams, for example, can ensure immediate investigation and remediation of data breaches. Businesses should also actively participate in industry self-regulatory organizations, collaboratively formulating and adhering to industry standards to elevate the overall data security level of the sector. Lastly, enterprises should willingly subject themselves to external regulatory oversight and public scrutiny, regularly disclosing data security reports to transparently showcase their data protection measures. Such transparency not only bolsters consumer trust but also encourages continuous self-improvement and enhancement within the enterprise. Data security is not merely a legal imperative; it is also a corporate social responsibility. Only by placing data protection at the forefront can enterprises thrive in the competitive market landscape and earn the enduring support and trust of consumers [5].

### *4.4. Enhance Consumer Personal Information Protection Awareness and Build a Multi-Dimensional Co-Governance Pattern*

In today's world, consumers frequently find themselves as direct victims of data breaches, yet many remain inadequately informed about the necessity and methods of personal information protection. This situation not only leaves the door open for unscrupulous individuals but also complicates the regulatory authorities' work. Therefore, it is imperative to initiate efforts from multiple avenues to enhance consumers' awareness of personal information protection. For instance, it would be beneficial to incorporate content on personal information protection into school education, fostering a cybersecurity awareness from a young age. This would enable children to understand the significance of their personal information and the potential risks of its exposure, while also equipping them with basic self-protection skills. The media should also shoulder the responsibility of public education by regularly publishing relevant news reports and 科普 articles, using vivid case studies and tangible data to alert consumers to the importance of personal information protection. Various social platforms and applications should provide clear privacy policy explanations during user registration and usage, utilizing pop-ups, message prompts, and other methods to inform users about how their personal information is handled and protected, ensuring that users can stay informed about their information status and make rational judgments and choices. Enterprises can further contribute by periodically conducting consumer personal information protection training to help users stay abreast of the latest protection technologies and methods. For example, workshops and interactive activities can be held both in offline stores and online platforms to address user queries and enhance their protection capabilities. Additionally, regulatory authorities should establish open and transparent complaint and reporting channels to encourage consumers to actively assert their rights when they encounter personal information leaks

or infringements. This could involve establishing specialized reporting portals on the official websites of consumer associations and regulatory bodies at all levels, simplifying the reporting process to ensure that reports are promptly addressed. Consumers themselves should actively learn relevant laws and regulations to understand their rights. Furthermore, they should cultivate good information management habits in their daily lives, such as regularly changing passwords, refraining from indiscriminately sharing personal information, and exercising caution when using public Wi-Fi. These measures not only enhance consumers' self-protection capabilities but also foster a societal consensus, enabling everyone to contribute to personal information protection in their daily lives. Ultimately, the formation of a multi-party collaborative governance framework necessitates the concerted efforts of government, enterprises, media, and consumers.

## 5. Conclusion

Although the current legal system has initially established a framework for protecting consumers' personal information rights, there are still numerous inadequacies in practical application. The lag of laws, the thinness of regulation, and the absence of corporate self-discipline place consumers in a relatively weak position. By improving relevant legislation to form a systematic legal system, strengthening administrative supervision to build a diversified regulatory mechanism, reinforcing corporate responsibility to establish a data security protection system, and enhancing consumers' awareness of personal information protection to foster a model of multiple stakeholders' governance, these measures will contribute to fundamentally addressing the issue of personal information protection. Only in this way can we better uphold consumers' personal dignity and legal rights in the age of informationization, and promote the harmonious development of society.

## References

1. M. Bębenek and B. Sypuła, "Discount as an example of a guarantee instrument in the field of the consumer's right to energy of an adequate quality," *Energies*, vol. 16, no. 4, pp. 1559–1559, 2023, doi: 10.3390/en16041559
2. Z. Luo, "Research on the innovation and improvement of civil and commercial law system facing e-commerce," *J. Econ. Law*, vol. 1, no. 4, pp. 11, 2024, doi: 10.62517/JEL.202414406
3. C. Mei, "Application of e-learning and new media teaching platform based on human-computer interaction technology in civil and commercial law courses," *Entertain. Comput.*, vol. 50, 100677, 2024, doi: 10.1016/j.entcom.2024.100677
4. Y. Ding, "Research on the protection of consumers' right to know in live streaming," *J. Sociol. Ethnol.*, vol. 5, no. 4, pp. 20, 2023, doi: 10.23977/jsoce.2023.050419
5. Q. Geng, "Innovative development path of e-commerce and civil and commercial law in the information age based on discrete regression algorithm," *Appl. Math. Nonlinear Sci.*, vol. 9, no. 1, pp. 18–19, 2024, doi: 10.2478/amns.2023.1.00379