

# The Legal Implications of Information Disclosure Obligations for E-Commerce Platforms: An Analysis Based on the Electronic Commerce Law of the People's Republic of China

Fenglin Liu<sup>1</sup>

<sup>1</sup> Nankai University, Tianjin, China

Correspondence: Fenglin Liu, Nankai University, Tianjin, China.

doi:10.56397/LE.2024.05.07

## Abstract

The Electronic Commerce Law (ECL) of the People's Republic of China is a pivotal regulation that imposes stringent information disclosure obligations on e-commerce platforms. This paper explores the legal implications of these obligations, focusing on their role in enhancing transparency, preventing fraud, and protecting consumer rights. It delves into the challenges faced by e-commerce platforms in complying with the ECL, particularly in terms of data privacy and dispute resolution. Through a comprehensive analysis, this paper provides recommendations for platforms to effectively navigate these challenges, ensuring compliance while fostering consumer trust and safeguarding user data. The findings highlight the importance of robust compliance measures and proactive strategies in building a trustworthy and secure e-commerce environment, ultimately contributing to the sustainable growth of the e-commerce sector in China.

**Keywords:** Electronic Commerce Law, information disclosure, data privacy, dispute resolution

## 1. Introduction

The advent of the digital age has revolutionized the way businesses operate, with e-commerce emerging as a dominant force in the global economy. This shift has been particularly pronounced in China, which boasts the largest e-commerce market in the world. The convenience and accessibility of online shopping have attracted millions of consumers, leading to exponential growth in the sector. However, this rapid expansion has also brought about significant regulatory challenges, necessitating the establishment of comprehensive legal frameworks to ensure fair and transparent operations within digital marketplaces.

Recognizing the need for a robust regulatory environment, the People's Republic of China enacted the Electronic Commerce Law (ECL) on August 31, 2018, which came into effect on January 1, 2019. The ECL is a milestone in the legal regulation of e-commerce in China, providing a comprehensive legal basis for the conduct of e-commerce activities. The law encompasses a wide range of issues, from market access and information disclosure to consumer protection and data privacy, reflecting the multifaceted nature of the digital economy.

One of the cornerstone features of the ECL is its stringent requirements for information disclosure by e-commerce platforms. These obligations are designed to enhance transparency and build consumer trust, which are critical components for the sustainable development of the e-commerce sector. Platforms are required to disclose a variety of information, including but not limited to, business registration details, product and service information, and transaction terms. The intent is to provide consumers with clear and accurate information, enabling them to make informed purchasing decisions.

Transparency is pivotal in e-commerce as it directly influences consumer trust and confidence. In an online environment where physical interactions are absent, the availability of reliable and accurate information is

paramount. The ECL's emphasis on information disclosure is aimed at addressing the asymmetry of information that often exists between consumers and online vendors. By mandating disclosure, the law seeks to mitigate risks associated with fraudulent activities and deceptive practices, thereby protecting consumer interests.

Consumer trust is a cornerstone of e-commerce success. Trust fraud, characterized by the manipulation of consumer trust for fraudulent gains, poses a significant threat to the integrity of e-commerce platforms. The ECL's disclosure requirements are integral to combating such fraudulent activities. By ensuring that consumers have access to necessary and truthful information, the law aims to foster a secure and trustworthy online shopping environment. This not only protects consumers but also benefits legitimate businesses by creating a level playing field.

In addition to information disclosure, the ECL addresses the resolution of disputes arising from e-commerce transactions. Online Dispute Resolution (ODR) mechanisms have been incorporated into the regulatory framework to provide an efficient and accessible means for resolving conflicts. However, these mechanisms come with their own set of legal implications, particularly concerning data privacy and procedural fairness. Ensuring that these online processes are just and unbiased is crucial for maintaining consumer confidence and upholding the principles of justice.

This paper aims to delve into the legal implications of information disclosure obligations as mandated by the ECL, analyzing their impact on various facets of e-commerce operations. It will explore the role of these obligations in fostering transparency and trust, preventing fraud, and facilitating dispute resolution. By examining the practical challenges and legal consequences faced by e-commerce platforms, this analysis seeks to provide a comprehensive understanding of the effectiveness and limitations of the ECL in regulating China's burgeoning e-commerce market.

## **2. Legal Framework of Information Disclosure**

### *2.1 Key Provisions of the Electronic Commerce Law*

The Electronic Commerce Law of the People's Republic of China stipulates several key requirements for information disclosure by e-commerce platforms. These include the obligation to clearly disclose business license information, product and service details, and transaction terms. The law aims to enhance transparency, ensure consumer protection, and establish a trustworthy e-commerce environment.

The ECL mandates that e-commerce operators provide comprehensive and truthful information about their products or services. This includes details about product specifications, pricing, delivery terms, and return policies. Such disclosures are intended to prevent misleading practices and ensure that consumers can make well-informed purchasing decisions (Standing Committee of the National People's Congress, 2018).

### *2.2 Trust and Fraud Prevention*

One of the primary motivations behind stringent information disclosure requirements is the prevention of trust fraud. Trust fraud has been identified as a significant challenge in China's e-commerce market, undermining consumer confidence and deterring online transactions. By mandating comprehensive disclosure, the ECL seeks to mitigate these risks and foster a more secure marketplace (Zhang et al., 2013).

Trust fraud typically involves the manipulation of consumers through the dissemination of false or misleading information. This can include fake product reviews, counterfeit goods, and deceptive pricing strategies. The ECL's provisions aim to curb such practices by ensuring that consumers have access to accurate and verifiable information about products and services. Enhanced transparency not only protects consumers but also deters fraudulent activities, thereby promoting a healthier e-commerce ecosystem (Zhang et al., 2013).

### *2.3 Dispute Resolution and Consumer Protection*

The ECL also addresses the mechanisms for online dispute settlement (ODS). While internal ODS models on e-commerce platforms are deemed effective, they cannot entirely replace traditional dispute resolution systems. Risks such as data leakage and lack of confidentiality persist, raising concerns about the fairness and impartiality of these processes. It is crucial for platforms to implement measures that protect procedural rights and maintain the integrity of dispute resolution processes (Ermakova, 2023).

The law requires that e-commerce platforms provide accessible and efficient mechanisms for resolving consumer disputes. These mechanisms are designed to handle complaints related to product quality, delivery issues, and other transactional conflicts. By offering streamlined dispute resolution processes, the ECL aims to enhance consumer protection and ensure that grievances are addressed promptly and fairly (Ermakova, 2023).

### *2.4 Data Privacy and Security*

Data privacy and security are paramount concerns in the context of information disclosure. E-commerce platforms must balance the need for transparency with the obligation to protect user data. Ensuring compliance

with both the ECL and data protection laws requires a comprehensive approach to data management, including robust encryption, secure storage, and stringent access controls.

The ECL mandates that e-commerce operators implement adequate measures to safeguard personal information and prevent data breaches. This includes obtaining explicit consent from users for data collection and usage, as well as providing clear and transparent privacy policies. By prioritizing data privacy, the law seeks to build consumer trust and confidence in the digital marketplace (Standing Committee of the National People's Congress, 2018).

### *2.5 Enhancing Consumer Trust*

Building and maintaining consumer trust is essential for the success of e-commerce platforms. Effective information disclosure practices, coupled with proactive measures to prevent fraud and ensure data security, can significantly enhance consumer confidence. Platforms should invest in technologies and processes that facilitate transparent and secure transactions, thereby fostering a trustworthy e-commerce environment.

To enhance consumer trust, e-commerce platforms should adopt best practices in information disclosure and data management. This includes providing detailed and accurate product descriptions, offering transparent pricing and return policies, and ensuring prompt and effective customer service. By prioritizing transparency and consumer protection, platforms can create a positive and trustworthy shopping experience (Zhang et al., 2013).

The Electronic Commerce Law of the People's Republic of China imposes stringent information disclosure obligations on e-commerce platforms, with significant legal implications. These requirements aim to enhance transparency, prevent fraud, and protect consumer rights. However, compliance with these obligations presents challenges, particularly in terms of data privacy and dispute resolution. By addressing these challenges and implementing robust compliance measures, e-commerce platforms can not only adhere to legal standards but also build a trustworthy and secure marketplace for consumers.

### **3. Legal Implications for E-Commerce Platforms**

E-commerce platforms operating in China are legally mandated to comply with the stringent information disclosure provisions outlined in the Electronic Commerce Law (ECL). These provisions require platforms to disclose comprehensive details about their business operations, including business licenses, product and service information, and transaction terms. The goal is to enhance transparency, protect consumer interests, and ensure that all necessary information is readily available and accurate.

Failure to adhere to these disclosure requirements can result in severe penalties. The ECL stipulates fines, business license revocation, and other administrative sanctions for non-compliant platforms (Standing Committee of the National People's Congress, 2018). For instance, platforms that fail to disclose essential business information or mislead consumers through false advertising can face substantial financial penalties. These punitive measures underscore the importance of compliance and serve as a deterrent against deceptive practices.

In addition to administrative penalties, e-commerce platforms may also be held liable for damages incurred by consumers due to inadequate or misleading information. This liability extends to various aspects of e-commerce operations, including product safety, service quality, and transactional integrity. For example, if a platform fails to disclose critical product information that leads to consumer harm, it could be sued for compensation. This legal framework places a significant compliance burden on e-commerce operators, necessitating robust internal mechanisms to ensure adherence to the law (Li & Huang, 2019).

To mitigate the risks associated with non-compliance, e-commerce platforms must develop and implement comprehensive internal compliance mechanisms. These mechanisms should include regular audits of business practices, continuous monitoring of information disclosure, and stringent quality control processes. Moreover, platforms should invest in training programs for employees to ensure they understand the legal requirements and the importance of accurate information disclosure.

The ECL also places significant emphasis on the resolution of disputes arising from e-commerce transactions. Recognizing the unique challenges posed by the digital marketplace, the law mandates the establishment of Online Dispute Resolution (ODR) mechanisms. These mechanisms are designed to provide an efficient and accessible means for consumers to resolve conflicts without resorting to traditional litigation, which can be time-consuming and costly.

While ODR models implemented by e-commerce platforms are generally effective in resolving disputes, they are not without their limitations. For instance, concerns about data leakage and lack of confidentiality persist, as ODR processes often involve the exchange of sensitive personal and transactional information. These issues can undermine the perceived fairness and impartiality of the dispute resolution process, potentially eroding consumer trust (Ermakova, 2023).

To address these concerns, the ECL mandates that e-commerce platforms implement measures to protect procedural rights and ensure the integrity of the dispute resolution process. This includes adopting secure data management practices, ensuring transparency in ODR proceedings, and providing consumers with clear information about their rights and the procedures for lodging complaints. By doing so, platforms can enhance the credibility and effectiveness of their dispute resolution mechanisms, thereby bolstering consumer protection.

Data privacy and security are critical components of the ECL's regulatory framework. Given the vast amounts of personal and transactional data handled by e-commerce platforms, the law imposes strict requirements for data protection. Platforms must implement robust security measures to prevent data breaches and unauthorized access, ensuring that consumer information is safeguarded at all times.

E-commerce platforms must comply with both the ECL and broader data protection regulations, such as the Cybersecurity Law and the Personal Information Protection Law (PIPL). These laws collectively establish a comprehensive legal framework for data privacy in China, requiring platforms to obtain explicit consent from consumers for data collection and use, provide transparent privacy policies, and implement effective data security measures (Standing Committee of the National People's Congress, 2021).

Building and maintaining consumer trust is essential for the success of e-commerce platforms. Effective information disclosure practices, coupled with proactive measures to prevent fraud and ensure data security, can significantly enhance consumer confidence. Platforms should invest in technologies and processes that facilitate transparent and secure transactions, thereby fostering a trustworthy e-commerce environment.

To enhance consumer trust, e-commerce platforms should adopt best practices in information disclosure and data management. This includes providing detailed and accurate product descriptions, offering transparent pricing and return policies, and ensuring prompt and effective customer service. By prioritizing transparency and consumer protection, platforms can create a positive and trustworthy shopping experience (Zhang et al., 2013).

The Electronic Commerce Law of the People's Republic of China imposes stringent information disclosure obligations on e-commerce platforms, with significant legal implications. These requirements aim to enhance transparency, prevent fraud, and protect consumer rights. However, compliance with these obligations presents challenges, particularly in terms of data privacy and dispute resolution. By addressing these challenges and implementing robust compliance measures, e-commerce platforms can not only adhere to legal standards but also build a trustworthy and secure marketplace for consumers.

#### **4. Challenges and Recommendations**

The implementation of the Electronic Commerce Law (ECL) of the People's Republic of China, while necessary for regulating the burgeoning e-commerce sector, presents several significant challenges that need to be addressed to ensure its effectiveness. This section explores these challenges and provides recommendations to overcome them, ensuring that e-commerce platforms can operate within the legal framework while maintaining consumer trust and protecting user data.

##### *4.1 Data Privacy and Security*

Data privacy and security are paramount concerns for e-commerce platforms, particularly in light of the ECL's stringent information disclosure requirements. Balancing the need for transparency with the obligation to protect user data is a complex task. Platforms must ensure that they comply with the ECL as well as other data protection laws such as the Cybersecurity Law and the Personal Information Protection Law (PIPL) (Standing Committee of the National People's Congress, 2021).

One of the primary challenges is implementing robust data management systems that can safeguard consumer information against breaches and unauthorized access. This requires investment in advanced encryption technologies, secure data storage solutions, and stringent access control mechanisms. Regular security audits and risk assessments are essential to identify vulnerabilities and address them promptly. Furthermore, platforms must develop comprehensive data privacy policies that clearly outline how user data is collected, used, and protected. These policies should be transparent and easily accessible to consumers, helping to build trust and ensure compliance with legal requirements.

To address these challenges, e-commerce platforms should adopt a proactive approach to data security. This includes employing cybersecurity experts to oversee data protection strategies, conducting regular training sessions for employees on data privacy best practices, and staying updated with the latest security technologies and regulatory changes. By fostering a culture of security and privacy, platforms can better protect consumer data and comply with legal standards.

##### *4.2 Enhancing Consumer Trust*

Building and maintaining consumer trust is crucial for the long-term success of e-commerce platforms. Effective information disclosure practices play a significant role in enhancing consumer confidence, as they ensure that

consumers have access to accurate and comprehensive information about products and services. However, mere compliance with disclosure requirements is not enough; platforms must also actively work to prevent fraud and ensure data security to foster a trustworthy environment.

One of the challenges in enhancing consumer trust is combating trust fraud, which undermines the integrity of the e-commerce ecosystem. Trust fraud involves deceptive practices such as fake reviews, counterfeit products, and misleading advertisements, which can erode consumer confidence. The ECL's stringent disclosure requirements aim to mitigate these risks, but platforms must go beyond legal compliance to implement effective anti-fraud measures (Zhang, Bian, & Zhu, 2013).

Platforms should invest in advanced fraud detection technologies that can identify and prevent fraudulent activities in real-time. These technologies can include machine learning algorithms that analyze transaction patterns, user behavior, and other indicators to detect anomalies. Additionally, platforms should establish robust verification processes for sellers and products, ensuring that only legitimate businesses and authentic products are available to consumers.

Transparency in business operations is another key aspect of building consumer trust. Platforms should provide clear and detailed information about their business practices, including pricing policies, return and refund procedures, and customer service protocols. By being transparent and responsive to consumer inquiries and complaints, platforms can create a positive shopping experience and enhance consumer trust.

#### *4.3 Recommendations for Effective Implementation*

To effectively implement the ECL and address the challenges discussed, e-commerce platforms should consider the following recommendations:

**Invest in Data Security:** Prioritize investment in advanced data security technologies and practices. Implement robust encryption, secure storage, and stringent access controls to protect consumer data. Conduct regular security audits and risk assessments to identify and address vulnerabilities.

**Develop Transparent Privacy Policies:** Create clear and accessible privacy policies that outline data collection, usage, and protection practices. Ensure that these policies comply with both the ECL and broader data protection regulations such as the Cybersecurity Law and PIPL.

**Implement Anti-Fraud Measures:** Invest in fraud detection and prevention technologies to combat trust fraud. Establish verification processes for sellers and products to ensure the authenticity and legitimacy of transactions.

**Enhance Consumer Engagement:** Foster transparency in business operations by providing detailed information about products, pricing, return policies, and customer service. Be responsive to consumer inquiries and complaints to build a positive and trustworthy shopping experience.

**Regular Training and Updates:** Conduct regular training sessions for employees on data privacy and security best practices. Stay updated with the latest regulatory changes and security technologies to ensure ongoing compliance and protection.

## **5. Conclusion**

The Electronic Commerce Law (ECL) of the People's Republic of China represents a significant milestone in the regulation of the digital marketplace, imposing stringent information disclosure obligations on e-commerce platforms. These requirements are fundamentally designed to enhance transparency, prevent fraud, and protect consumer rights, thereby fostering a more secure and trustworthy e-commerce environment. However, the implementation of the ECL is not without its challenges, particularly in terms of data privacy and dispute resolution, which necessitate comprehensive and proactive compliance measures.

One of the core objectives of the ECL is to enhance transparency within the e-commerce sector. By mandating detailed information disclosure about business licenses, product specifications, and transaction terms, the law aims to address the information asymmetry that often exists between consumers and online vendors. This transparency is crucial for building consumer trust, as it allows consumers to make informed purchasing decisions based on reliable and comprehensive information. In this context, the law acts as a safeguard against deceptive practices such as false advertising and counterfeit products, which have plagued the e-commerce market (Standing Committee of the National People's Congress, 2018).

Preventing fraud is another critical aspect of the ECL. Trust fraud, which involves the manipulation of consumer trust through deceptive means, poses a significant threat to the integrity of the e-commerce ecosystem. The ECL's stringent disclosure requirements serve as a deterrent against such fraudulent activities by ensuring that consumers have access to accurate and verifiable information. This legal framework not only protects consumers but also promotes fair competition among businesses by creating a level playing field (Zhang, Bian, & Zhu, 2013).

Despite these benefits, compliance with the ECL presents considerable challenges, particularly in the realms of data privacy and dispute resolution. E-commerce platforms handle vast amounts of personal and transactional data, making data privacy and security paramount concerns. The law requires platforms to implement robust security measures to safeguard this data, which involves significant investment in advanced technologies and comprehensive data management practices. Ensuring compliance with the ECL and broader data protection regulations, such as the Cybersecurity Law and the Personal Information Protection Law (PIPL), is essential for protecting consumer information and maintaining trust (Standing Committee of the National People's Congress, 2021).

Dispute resolution is another area where the ECL's implementation poses challenges. The law mandates the establishment of Online Dispute Resolution (ODR) mechanisms to provide efficient and accessible means for resolving consumer conflicts. However, concerns about data leakage and the lack of confidentiality in ODR processes can undermine their effectiveness and fairness. E-commerce platforms must therefore adopt secure data management practices and ensure transparency in ODR proceedings to protect procedural rights and maintain consumer confidence (Ermakova, 2023).

To navigate these challenges, e-commerce platforms need to adopt a proactive approach to compliance. This includes investing in advanced data security technologies, developing transparent privacy policies, and implementing effective fraud detection and prevention measures. Moreover, platforms should engage in continuous training and education for their employees to ensure they are well-versed in legal requirements and best practices for data protection and consumer interaction.

In conclusion, the ECL's stringent information disclosure obligations have far-reaching legal implications for e-commerce platforms. While these requirements aim to enhance transparency, prevent fraud, and protect consumer rights, they also present significant compliance challenges. By addressing these challenges through robust compliance measures and proactive strategies, e-commerce platforms can not only adhere to legal standards but also build a trustworthy and secure marketplace. This, in turn, will foster consumer confidence and contribute to the sustainable growth of the e-commerce sector in China.

## References

- Chen, X., & Wang, C, (2022). Online arbitration of e-commerce disputes in the People's Republic of China: Due process concerns. *Chinese Review of International Law*, 8(2), 1-25. Retrieved from [http://cwr.yiil.org/home/pdf/archives/2022v8n2/cwr\\_v8n2\\_01.pdf](http://cwr.yiil.org/home/pdf/archives/2022v8n2/cwr_v8n2_01.pdf)
- Ermakova, E, (2023). Features of online settlement of consumer disputes by e-commerce platforms in the People's Republic of China. *Journal of Digital Trade Law*. Retrieved from <https://www.lawjournal.digital/jour/article/download/242/61>.
- Feng, S., Wan, Y., & Fang, F, (2019). Notice and take down: How the shift from copyright law to Chinese e-commerce law poses an unnecessary disturbance to e-commerce. *International Journal of Law and Technology*, 28(4), 505-525.
- Li, X., & Huang, W, (2019). The E-commerce Law of the People's Republic of China: E-commerce platform operators liability for third-party patent infringement. *Computer Law & Security Review*, 35(6), 105347.
- Standing Committee of the National People's Congress, (2018). Electronic Commerce Law of the People's Republic of China. Retrieved from <http://www.npc.gov.cn/englishnpc/c23934/201812/245eaa1a5b3c4f2ab833b67b9238e28a.shtml>.
- Standing Committee of the National People's Congress, (2021). Personal Information Protection Law of the People's Republic of China. Retrieved from <http://www.npc.gov.cn/englishnpc/c23934/202109/c0b5db1af40e4b1cbcb3c31e9bdef24b.shtml>.
- Zhang, Y., Bian, J., & Zhu, W, (2013). Trust fraud: A crucial challenge for China's e-commerce market. *Electronic Commerce Research and Applications*, 12(5), 299-308.

## Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).