ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

Research on Consumer privacy protection of e-commerce platform—Empirical analysis based on the privacy clauses of 20 e-commerce platforms

Cao Yi

Anhui University of Finance and Economics (Longhu West Campus), Bengbu, Anhui, China, 233000

Abstract: *With the rapid development of online shopping in China, e-commerce platform, as the shopping channel that consumers often rely on, has been paid more and more attention. However, the privacy clauses that platforms require consumers to sign before providing services are related to the protection of privacy rights in online consumption. Through empirical and theoretical studies, it is known that there are defects in consumers' negotiating position, privacy information sharing channels and subject responsibility. Therefore, it is better to strengthen the inclined protection of "informed consent". Strengthening fiduciary duty and introducing third party evaluation mechanism to strengthen privacy protection.*

Keywords: *Consumer Rights and Interests, Privacy Right, E-commerce Platform, Privacy Policy*

1. Introduction

According to the "China E-commerce Report (2021)" released by the Department of E-commerce and Information Technology of the Ministry of Commerce, the national e-commerce transaction volume reached 42.3 trillion yuan in 2021, a year-on-year increase of 19.6%, of which the transaction volume of commodities reached 31.3 trillion yuan and the service transaction volume reached 11 trillion yuan. In online consumption represented by e-commerce, merchants usually need to collect consumers' personal information for commercial operation and push business, but there is a large amount of privacy data closely related to consumers' vital interests in this personal information. In order to give full play to the advantages of the entity, avoid business risks and better protect the privacy of consumers, most online consumer platforms have formulated privacy clauses, most of which cover information collection, use, storage, protection, sharing, and the protection of minors. Privacy infringement disputes brought about by online consumption and the development of platform economy have become a major pain point in the protection of consumer rights and interests.

2. Legal basis of Privacy Clauses of e-commerce platforms

2.1. The basic connotation of the Privacy Clause

Privacy terms refer to the relevant rules expressed by software service providers regarding the rights, obligations and responsibilities for the protection of users' privacy and security[1]. An e-commerce platform means an information platform for buyers and sellers to match, conclude transactions and provide relevant services through information network technology[2]. According to the 50th Statistical Report on the Development of the Internet in China, by June 2022, the number of online payment users in China has reached 904 million, online shopping users have reached 841 million, and online travel booking users have reached 333 million, among which online payment and shopping users account for more than 80% of the total number of netizens. As the Internet era arises at the historic moment, the online consumption platform is an important innovation of consumption means. Under the guidance of policies to expand consumption and encourage the healthy development of platform economy, e-commerce platforms are increasingly playing an increasingly important role in China's economy. In the early stage of the development of Internet commerce, the form of privacy clauses is more abundant, such as consumer agreement, service agreement, usage instructions and other related documents and materials. However, with the rapid development of online consumption and the improvement of the national rule of law, privacy clauses have gradually become an important content of e-commerce platforms. And has formed an independent privacy policy release form and display options on multiple platforms. At present,

ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

the privacy terms of China's e-commerce platforms are generally nested in their mobile clients or web terminals. For example, the way to query the privacy terms of Anjuke platform for residential e-commerce is as follows: APP- about Anjuke - Anjuke privacy policy. For more complicated ones, the way to query the privacy terms of Douyin platform for sharing e-commerce platform is as follows: APP- My - three horizontal lines on the upper right - Settings - Privacy Policy - "Douyin" Privacy Policy Brief version - Privacy Policy. For enterprises, the privacy policy can not only fulfill the obligation of notification, but also restrict their own behavior and cooperate with supervision and management; For consumers, privacy clauses can not only protect their privacy, but also provide evidence to support when their privacy rights are violated. [3]

In the network environment, privacy policy-based privacy protection mainly constrains the content and way of collecting personal information by Internet service providers through privacy policies, controls the use method of the collected information, and grasps the use of the collected information, so as to protect personal privacy. In order to solve the problem of how to make more effective use of information and ensure that the information does not violate the user's privacy in the application process, scholars have been committed to studying the privacy protection mechanism based on privacy policy, in order to achieve a balance between the two aspects. Starting from this purpose, some scholars have adopted empirical analysis methods and means to explore the existing problems of privacy policies. How to cultivate the privacy clauses of third-party applications and other studies have found that currently a considerable number of application privacy clauses lack operability and compliance, so it is necessary to continue to explore and improve the privacy security mechanism of mobile phone users. If other methods can be combined in the empirical analysis, it will be more strategic. For example, Liu Bailing et al. concluded the concept of "privacy element" by studying empirical analysis literature and forming a review. They believed that privacy element was a meta-component of privacy policy, and combined them according to specific circumstances, constituted the content of privacy policy. The reason why researches on privacy clauses of e-commerce platforms have attracted long-term attention of scholars is that there is a distance between the practice of consumer privacy protection on platforms and the protection of privacy by law. Various research means are needed to promote the improvement of privacy clauses and the implementation of relevant commitments. [4]

2.2. Analysis of the nature of privacy clauses

According to the current privacy clauses of mainstream e-commerce platforms, privacy clauses should be considered as a kind of network contract requiring the "consent" of consumers. [5]In terms of content, one party (consumers) assigns part of the right to personal information in order to obtain the convenience of use, and the other party (e-commerce platform) promises to implement strict protection responsibilities while using consumer information legally. That is, it forms a structure in which one party makes an offer and the other party promises, which conforms to the provisions of the Civil Code on the typical way of contract establishment. The format contract signed in the form of network has the advantages of high efficiency, convenience and traceability. At the same time, the risk can be fixed in advance to reduce the operational risk of the e-commerce platform, which is also in line with the characteristics of the platform itself. However, just like the emerging consumption mode of online consumption, the network format contract of privacy clause launched by the e-commerce platform also has natural defects, such as excessive virtuality and strong technology. [6] Virtuality means that the background, process of negotiation and way of presentation of privacy clauses are carried out and completed in a virtual environment, which will to a large extent reduce the caution and personal experience of consumers in signing, and objectively cause consumers to pay less attention to their own rights and interests. Technicality means that the opening and reading of privacy clauses requires a certain level of technology to be completed substantively, that is, higher cultural quality requirements are put forward for consumers. According to the 46th Statistical Report on the Development of Internet in China released by China Internet Network Information Center (CNNIC) in September 2020 (hereinafter referred to as the Report), 59.7% of netizens with an education level below junior high school (including), and according to the 50th report released in August 2022, The proportion of Internet users over 50 years old has reached 25.8%, and the number of older users keeps rising with the acceleration of aging. As a result, it is difficult for a considerable number of online consumers to reach the technical level required to read the privacy clauses, which effectively results in the difficulty of protecting their rights and interests.

ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

3. Empirical research on privacy clauses of e-commerce platforms

3.1. Research sample of privacy policy

Based on the ranking documents issued by webmaster's Home (www.chinaz.com) and other third-party institutions, as well as the actual popularity of their use, this paper selected 23 privacy terms data of e-commerce platforms for empirical analysis, carefully considering the representativeness of the platforms, the comprehensiveness of the types and the timeliness of the terms. It can reflect the nature of the research object in this paper more completely and scientifically. The platform covers seven categories, including shopping, catering, ticket, travel, payment, residence and sharing, and the terms are all from the latest content released by the platform itself. Shopping platforms include Jingdong, Taobao, Pin-Duo, Xianyu, etc.; catering platforms include Ele. me, Meituan, Meituan Takeout, Koubei, etc.; ticketing platforms include Maoyan Film, Damai, Taopiaopiao, etc.; travel platforms include Feizhu, Zhixing, Ctrip, etc.; payment platforms include Alipay, wechat Pay, Yunshanpay, etc.; living platforms include Huao.com, Lianjia, etc. Anjuke, and sharing platforms include Zhihu, Douyin, Xiaohongshu, Kuaishou, etc. (See Table 1) According to the collected information, the major e-commerce platforms generally set their business focus on the mobile terminal at present, and the privacy terms of some platforms can only be viewed on the mobile terminal. Therefore, except for the general situation, the information on the mobile terminal shall prevail. On the basis of the preliminary understanding of the privacy clauses, the survey and processing of the data adopts the subject-oriented approach and analyzes the three aspects of the anchoring clauses, namely, the negotiating position of consumers, the propagation path of privacy information, and the main responsibilities of protection obligations, which is more conducive to improving the pertinence of the empirical research.

3.2. Sample content analysis of privacy policy

3.2.1. Overview

After empirical research, it can be seen that the privacy policies of mainstream e-commerce platforms are mostly named "privacy policy", "privacy clause", "personal information protection policy", etc., and the update time is relatively close to the research time (see Table 1).

Table 1 E-commerce platform privacy policy summary table

Type of platform	Platform name	Term name	Update time
Generics	JD.com	Jd.com Privacy Policy	Oct 19, 2022
	Taobao	Taobao.com Privacy Policy	Dec 9, 2022
	Pinduoduo	Pinduoduo Privacy Policy	April 7, 2022
	Idle Fish	Leisure Fish Community Privacy Policy	December 7, 2022
Food and Beverage category	Hungry	Ele. me privacy policy	November 18, 2022
	Meituan	Meituan Privacy Policy	March 14, 2022
	Meituan Takeaway	Meituan Takeaway Privacy Policy	November 04, 2021
	Word of Mouth	Word-of-mouth privacy protection policy	June 23, 2022
	Dianping	Dianping Privacy Policy	June 2, 2022
Ticketing category	Cat's Eye movie	Maoyan Platform Privacy Policy Summary	January 17, 2023
	Tao Piao Ticket	Taopiaopiao Privacy Policy	November 30, 2022
	Barley	Barley Privacy Policy	November 25, 2022
Travel Category	Chi Xing	Chi Heng Personal Information Protection Policy	29 November 2022
	Flying Pig	Flying Pig Privacy Policy	December 2, 2022
	Ctrip	Ctrip personal information protection policy	June 23, 2022
Payment Category	Alipay	Alipay Privacy Policy	July 14, 2022
	wechat	Wechat Privacy Protection guidelines	June 27, 2022
	Cloud Flash Payment	Cloud Flash Pay Privacy policy	November 30, 2022
Residential Category	Shell house hunting	Shell Privacy Policy	September 19, 2022
	Lianjia	Homelink Privacy Policy	Unclear
	Anjuke	Anjuke Privacy Policy	June 24, 2022
Share Class	Zhihu	Guidelines on Personal Information Protection	29 October 2021
	Tiktok	"Douyin" privacy policy	November 30, 2022
	Little Red Book	Xiaohongshu User Privacy Policy	April 30, 2022
	Fast hand	Privacy protection policy	December 18, 2022

ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

3.2.2. Consumer negotiated bargaining position

Table 2 E-commerce platform privacy clause consumer negotiation negotiation position analysis table

Type of platform	Platform name	Whether as a pre-condition for consumer registration	Whether it is accompanied by a concise version	Whether a telephone answering service is provided	Whether you provide an online question-answering service	Number of inquiries	
						Web side	Mobile
Generics	JD.com	√	√	√		2	5
	Taobao	√	√	√		2	5
	Pinduoduo	√	√	√		2	5
	Idle fish	√	√	√		No data	5
Catering category	Hungry	√	√	√		2	5
	Meituan	√	√	√		2	5
	Meituan Takeout	√	√	√		No data	5
	Word of mouth	√		√		No data	5
	Dianping	√	√	√		4	5
Ticket category	Cat eyes	√	√	√		2	7
	Scour tickets	√				2	6
	Barley	√	√	√		2	5
Travel Class	Chi Xing	√		√	√	No data	5
	Flying Pig	√	√	√		2	5
	Ctrip	√	√	√		2	4
Payment class	Alipay	√		√		3	5
	wechat	√	√	√		2	5
	Cloud flash payment	√		√		3	5
Residential category	Shells	√	√	√		No data	5
	Lianjia	√	√	√		2	5
	Anjuke	√	√	√		3	4
Share classes	Zhihu	√	√	√		2	5
	Tiktok	√	√	√		2	7
	Little Red Book	√	√	√		2	5
	Kuaishou	√	√	√		3	5

In the part of negotiating position of consumers, we mainly examine the "friendliness" of privacy clauses to consumers (see Table 2). As we all know, consumers often cannot fully enjoy their consumption rights due to their natural disadvantages in trading position, and the most prominent of these "disadvantages" is the disadvantage in negotiating position. For example, some scholars think that some contents of the privacy clause are vague and difficult to identify. And strong tendency and orientation (Chen Shiyang, Liu Tingting, 2020). [7]

As can be seen from the above table, at present, various e-commerce platforms generally regard consumers' "consent" to privacy terms as a prerequisite for their registration as platform users, which is generally displayed in a prominent position on the login interface when consumers enter the software for the first time in the form of highlighting. In order to create conditions in the form that consumers may read, by January 2022, 18 of the 23 platforms in the table have provided concise versions of the privacy terms, while Koubei, Taopiaopiao, Zhixing, Alipay, Cloud Flash Pay and other platforms have not yet provided them. At present, in addition to the Chi Xing platform, the major e-commerce platforms generally adopt a relatively simple telephone mode (which is matched with email, offline mode) for feedback, and rarely use the currently mature online customer service question answering method. In terms of the number of inquiry links, 87% of platforms have 5 inquiry links, and the number ranges from 4 to 7. The number of inquiry links on the mobile terminal is generally more than that on the web terminal.

ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

3.2.3. Propagation path of privacy information

Table 3 E-commerce platform privacy policy information sharing analysis table

Platform type	Platform name	Purpose of communication	Extent of transmission	Transmission path
General classes	JD.com	√	√	√
	Taobao	√	√	√
	Pinduoduo	√	√	√
	Idle fish			
Catering category	Hungry	√	√	√
	Meituan	√	√	√
	Meituan Takeout	√	√	√
	Word of mouth	√	√	√
	Yelp	√	√	√
Ticket class	Cat's Eye movie	√	√	√
	Amoy ticket	√	√	√
	Barley	√	√	√
Travel class	Chi Xing	√	√	√
	Flying Pig	√	√	√
	Ctrip	√	√	√
Payment class	Alipay	√	√	√
	wechat	√	√	√
	Cloud flash pay	√	√	√
Residential category	Shell house hunting	√	√	√
	Homelink	√	√	√
	Anjuke	√	√	√
Share classes	Zhihu	√	√	√
	Tiktok	√	√	√
	Little Red Book	√	√	√
	Kuaishou	√	√	√

The main purpose of the privacy policy itself is to protect consumers' privacy and other personal information, but e-commerce platforms usually list the circumstances under which they need to share information based on business needs. As a way to share and circulate private information, the transmission path plays a key role in protecting the right to privacy. In addition, there are often additional situations in which private information can be shared and disseminated without informing consumers, such as information based on judicial, administrative, national security, public security, epidemic prevention and control, and information needed to protect the life, property and other major legitimate rights and interests of the subject of personal information or other individuals, but difficult to get consent from the person, public report, etc. As a leading food delivery enterprise, Meituan Takeout platform clearly defines the purpose of information sharing as "to provide platform services", "to provide unified management services", "to provide necessary cooperation services", "to ensure safety and optimize services" and "to provide services based on legal circumstances". Zhixing occupies a large market share among the current travel platforms. Its scope of communication is limited to suppliers, financial institutions, third-party payment institutions, business partners, affiliated companies, credit investigation agencies, etc., and the scope of sharing is also clearly stipulated. Zhihu, on the other hand, puts forward four communication paths in its Personal Information Protection Guidelines, including "entrusted processing," "sharing", "transfer" and "public disclosure". It is worth noting that Maoyan, a mainstream platform of ticket economy, has put forward three information sharing principles in its privacy terms, namely, "Principle of authorization and consent", "Principle of legality and minimum Necessity", and "principle of security and prudence"(see Table 3).

3.2.4. The main responsibility of the protection obligation

The clear protection responsibility is an important support for the protection of consumer privacy, among which the platform itself, the third party and the government play a crucial role. According to the research, most mainstream e-commerce platforms have listed their measures to protect consumers' privacy information, preset security "levels" and plans for related security events in their privacy clauses(see Table 4), which basically cover the following aspects: (1) Technical measures and data security measures: The establishment of data classification and classification system, data security management norms, data security development norms to manage the storage and use of personal information, to ensure that there is no collection of personal information unrelated to the services it provides. At the same time, the platform will also conduct comprehensive security control over data by signing confidentiality agreements with information contacts, monitoring and auditing mechanisms.

ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

Prevent unauthorized access, public disclosure, use, modification, damage or loss of personal information. (2) Security certification: The platform usually passes the information security level protection certification of the Ministry of Public Security to strengthen the management of security identification authority. (3) Security incident handling: It mainly includes informing consumers in time once a security incident occurs, so that consumers can independently prevent and remedy it. This part belongs to the bottom protection measures. However, it is not difficult to find that e-commerce platforms seldom touch on the third-party intervention mechanism and government supervision mechanism in the privacy clauses, but tend to emphasize their own protection measures in a longer length. It is worth mentioning that when describing its means of consumer personal information protection, Feizu Platform mentioned: "If you are worried about your personal information, especially your account or password, please contact Ali 110 immediately to complain or contact Feizu customer service, so that we can take corresponding measures according to your application." After investigation, it was found that the "Ali 110" here should be the Ali Security Center of the Ali Alliance, and according to the Sky Eye check system showed that the trademark of "Fei Zhu" is the brand of Alibaba Holding Group Co., LTD., it can be identified that Alibaba has substantial control over the Fei Zhu platform, so the "Ali 110" here cannot be identified as a third-party supervision mechanism. Although some platforms such as cloud Flash Pay mentioned will "in accordance with laws and regulations and regulatory requirements, take the initiative to report the disposal of personal information security incidents", but did not explain the responsibilities of the regulatory authorities and specific names, can only be formalized as a statement. Most platforms generally indicate in the security measures that they have been rated by the Ministry of Public Security or a third party platform. Kuaishou platform clearly states that it has "passed the third-level information security protection certification, and passed the international authoritative ISO27001 information security certification and ISO27701 privacy information management certification", but it still cannot be regarded as a clear third party regulatory responsibility. More can not be regarded as a clear complaint channel for government departments.

Table 4 E-commerce platform privacy policy entity responsibility analysis table

Type of platform	Platform name	Whether the platform's protection responsibilities are stated	Whether the third party's protection responsibilities are clearly defined	Whether the path to complaint to a government department is clear
General Categories	JD.com	√		√
	Taobao	√		
	Pinduoduo	√		
	Idle fish	√		
Dining category	Hungry	√		
	Meituan	√	√	
	Meituan Takeout	√	√	
	Word of mouth	√		
	Yelp	√		
Ticket category	Cat's Eye movie	√		
	Amoy ticket	√		
	Barley	√		
Travel class	Chi Xing	√		
	Flying Pig	√		
	Ctrip	√		
Payment class	Alipay	√		
	wechat	√		
	Cloud flash pay	√		
Residential category	Shell house hunting	√		
	Homelink	√		
	Anjuke	√		
Share classes	Zhihu	√		
	Tiktok	√		
	Little Red Book	√		
	Kuaishou	√		

4. Problems in the privacy clauses of e-commerce platforms

4.1. Lack of negotiation and dialogue mechanism

As a kind of contract, privacy clause should provide convenient and equal negotiating position to achieve mutual agreement and protect the fairness of the transaction. As for the privacy clause itself, the

ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

convenience of access is related to the possibility of consumers knowing the protection of their rights. As far as the mobile terminal is concerned, the access to the privacy clause is divided into the access at registration and the access after registration. Before registration, consumers often need to formally recognize the agreement to continue the registration and login operation. However, due to the lack of time in registration, more than 80% of the respondents in this small survey said that they would not read the privacy terms when registering new users on e-commerce platforms (see Figure 1). Searching after registration provides consumers with a way to remedy their rights, but the survey shows that 90% of respondents do not read the terms after registration (see Figure 2).

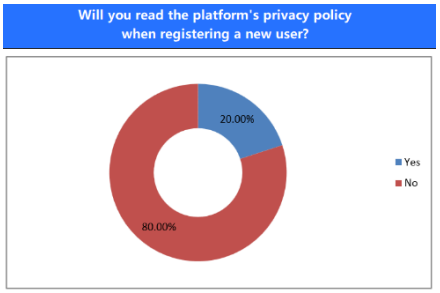

Figure 1:Chart of how consumers read privacy terms

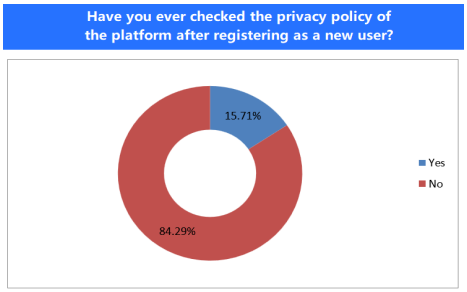

Figure 2:Statistical chart of consumers reading privacy terms after e-commerce platforms

If few consumers read the privacy terms carefully before registration due to time constraints, however, few consumers still read the terms in a relatively loose time after registration, there should be other explanations, such as poor access convenience, high difficulty in reading, limited auxiliary means, etc. The number of links to query the terms in terms of convenience is a data element less concerned by the academic community at present, but it is crucial to the realization of consumer privacy rights. The complexity of the way to read the privacy terms is also a major factor affecting whether the privacy terms can actually be read by consumers. At present, the number of links to consult the privacy terms on the mobile terminals of most mainstream e-commerce platforms is more than 4 times, and the number of links to query the privacy terms on Douyin platform is as high as 7 times. The excessive search links of privacy terms lead to a hidden state, which makes it difficult for consumers to notice the existence of the terms in daily use, let alone consult the contents of the terms. At the same time, the cumbersome procedures also cause consumers even if they know the existence of the terms will also because of inertia and not to consult. Poor understanding of the necessity of reading privacy terms after registration may also be one of the influential factors that consumers almost don't read terms. The difficulty of reading the terms is based on the more text and more professional expression of the terms, so many e-commerce platforms provide a concise version of the privacy terms for consumers to consult, but the content of the concise version of the terms is sometimes too simple and simple. At the same time, whether the concise version of the privacy clause itself can have the same legal effect as the detailed version of the privacy clause remains to be verified. Privacy clauses are not the services provided by e-commerce platforms, nor can they provide the content that consumers urgently need. Consumers often do not have the habit and motivation to consult privacy clauses, and the question answering service is an active intervention to protect consumers' right to privacy, that is, the process of answering questions when consumers have questions about privacy clauses. This process can significantly reduce the difficulty of consumers' understanding of the terms themselves and the difficulty of knowing the platform's means of privacy protection, and draw the distance between the platform and consumers through positive interaction. However, according to empirical research, currently e-commerce platforms generally use their own contact phone numbers and address listed in the privacy terms as the contact channel, in sharp contrast to this is that major e-commerce platforms often provide convenient online question-answering services in the pre-sale service advisory window marked with purchase in the prominent position of the services or commodities they provide. Online customer service contact has the advantages of convenience, immediacy, leaving traces, etc., which are not possessed or lacking by telephone contact, postal contact or even offline contact.

4.2. Information sharing rules are vague

According to the results of the empirical study, the mainstream e-commerce platforms generally list the way of information sharing path in the privacy clause, and the form also covers the purpose, scope and path. According to the Personal Information Protection Law, the processing of personal information includes "collection, storage, use, processing, transmission, provision, disclosure, deletion, etc." Means,

ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

its collection should be limited to the "minimum limit", it can be seen that China's special legislation has been strictly grasp the collection and dissemination of personal information standards, but how to implement the legislative requirements to the e-commerce platform, how to open up the "last mile" of privacy protection needs to be further thought. Compared with the legal provisions themselves, more closely related to the vital rights and use experience of consumers are the norms on which enterprises (e-commerce platforms) directly provide services or commodities. If the requirements for information sharing rules can be further refined on the basis of the current privacy policy, it will be more beneficial to the protection of privacy rights. At present, the requirements of information sharing rules in mainstream e-commerce platforms are abstract and fuzzy, with a low degree of systemization. For example, the privacy policy of Jingdong lacks the principle of information sharing, and the privacy clause of Koubei lacks the specific situation of the platform sharing information with partners. At the same time, a few platforms are more systematic and detailed in the rules of information sharing. For example, in the privacy policy of Damai Platform, the use of information (" use "means sharing with partners based on the content of the provisions) includes" basic principles ", "scope of partners", "entrusted processing", "joint processing", "cooperation scenarios" and other contents. The arrangement logic is more rigorous in accordance with the "total-division" structure. Meanwhile, the "Contract scenario" section of the platform lists specific possible situations of information sharing in detail. For example, Douyin platform has added process rules on how to deal with the deceased's information into the terms, which further improves the system of information processing and sharing, and at the same time enhances the humanization level of platform operation. In particular, it is worth noting that user information sharing exists under the special situation that the privacy policies of different platforms belonging to the same enterprise allow the sharing of user information. This is called the information aggregation effect of Internet giant companies, which is very obvious in the e-commerce groups with large scale and many holding companies. [8]For example, Beijing Sankuai Online Technology Co., Ltd. owns Meituan, Meituan Waimai, Dianping and other platforms, while Alibaba Group Holding Co., Ltd. owns dozens of e-commerce platforms such as Taobao, Alipay, Xianyu, Feizhu, Ele. me and Koubi. These e-commerce platforms belonging to the same enterprise show the characteristics of clustering, and their business strategies and privacy policies are also highly similar. Some of the terms are even completely similar.

4.3. The main protection function fails

"Personal information handlers are the first responsible person for personal information protection" and network operators are the first responsible person for personal information protection. The emphasis on operators' responsibility has been frequently seen in Chinese laws, including the Cyber Security Law implemented in 2017 and the Personal Information Protection Law issued in 2021. In the "Network security Law", the relevant expression is "network operators shall keep the user information collected strictly confidential, and establish and improve the user information protection system", in the "Personal information Protection Law", the relevant expression is "personal information processing operators shall be responsible for their personal information processing activities, and take necessary measures to ensure the security of the personal information handled", By comparison, it is not difficult to find that the concept of "personal information processor" in the Personal Information Protection Law has a wider scope and can include merchants and e-commerce platforms in terms of the meaning, which can better adapt to the needs of economic development of Chinese platforms. The privacy clauses of mainstream e-commerce platforms also generally emphasize the main responsibility of platforms and settled merchants for the protection of consumer privacy, which is inseparable from the repeated emphasis of legal provisions and the society's high attention to personal information processors. However, in recent years, there has been an increasing number of cases in which consumer privacy has been disclosed. It is urgent to further strengthen the main responsibility of consumer privacy protection, and the privacy clause, as an important basis for privacy protection, needs to be improved in this aspect. At present, in the privacy clauses of mainstream e-commerce platforms, the protection responsibility of the platform is longer than the concept and commitment, but shorter than the supervision and implementation. Often, a large number of professional terms are piled up to indicate that the privacy protection level of the platform has passed the third-party assessment or reached a certain national standard, but the platform is still in the stage of relying on the concept endorsement. In terms of third-party evaluation, most privacy clauses still regard it as an accessory of platform responsibility rather than an independent supervision procedure. For example, Ctrip states in the fifth part of the clause that its protection technology "has obtained ISO27001 information security management system standard certification and PCI-DSS payment card industry data security standard certification". For example, Meituan Takeout said that it has "passed the Ministry of Public Security information security level protection level three certification, ISO27001 information security certification, third-party payment industry (payment card industry PCI DSS) data

ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

security standard international certification qualifications". In terms of the intervention of government departments, the vast majority of provisions do not have specific provisions, generally do not list the complaint organization, but also do not show the complaint channel and contact information, if the consumer in the case of fruitless negotiation to seek the assistance of the government departments, they need to search and query again, which increases the cost of consumer rights protection.

5. Solutions to online consumer privacy protection problems

5.1. Strengthen slanting protection under the principle of "informed consent"

5.1.1. The correct application of the informed consent principle

The principle of informed consent refers to the principle that an information provider should fully inform the information subject about the collection, processing and utilization of relevant personal information and obtain the explicit consent of the information subject when collecting personal information. [9]In other words, the principle of informed consent is a restatement of the contractual attributes of privacy clauses, while the emphasis on informed consent is also an affirmation of consumers' "right to consent". Some scholars believe that the freedom of decision of the information subject of personal information is "not real" and difficult to achieve, but just as the British classical empiricism philosopher John Locke said in the "Theory of Government" : "people are born free, equal and independent, without their consent, no one can be put out of this state", consumers to grasp the right to consent itself is also an important freedom[10]. The principle of informed consent and all kinds of "informed agreements" derived from it can be fully applied on the basis of value measurement and correct judgment in law enforcement and judicature. Consumers have the right to "consent" to the right to privacy in the negotiation. [11]The General Data Protection Regulation also stipulates that "consent" is the legal basis for data processing. [12]Like other legal principles, the application of the principle of consent requires attention to the way of notification, the way of consent and the scope of application of the principle.

1) At present, the notification of privacy terms on e-commerce platforms is mainly displayed in the form of electronic text directly on mobile terminals or web terminals, while the consent is mainly by consumers checking "I have read and agree". According to empirical research, the display of privacy terms on mainstream e-commerce platforms is still too simple. Although the concise version of the clause has been popular, it is still mainly in the form of text, and the contact information is still mainly in the form of telecommunications. The platform can innovate the way of displaying the clause, and add flexible and vivid display means such as pictures, forms, videos, audio, etc. At the same time, full-time positions such as compliance specialists can be set up to meet online customer service staff to service consumers' questions about the privacy terms. In a word, e-commerce platforms should create conditions for consumers to fully understand the privacy terms to the maximum extent.

2) From the perspective of content, the privacy clause is not monolithic. The privacy information data involved includes not only the nickname, user name, profile picture and other general indicative information of consumers, but also the behavior, operation path, geographical positioning, public interaction and other information, as well as the key information such as assets, physical health, etc. For different types of information, there should be different ways of "consent". According to the EU's General Data Protection Regulation (GDPR), consumers have the right to object to the handling of sensitive data, direct marketing and user portraits, which puts more emphasis on protecting users' data. For general information that does not concern consumers' personal interests, the platform should allow consumers to allow extraction and use of such private information by default based on transaction efficiency and consumption experience. For general privacy that does not involve sensitive information, opt-out consent mode should be adopted to allow consumers to choose out the privacy that they think should not be authorized to be used by the platform, which not only ensures efficiency but also fully protects consumers' right of choice. For sensitive information, opt-in consent should be adopted, focusing on the protection of consumer privacy, and consumers have the right to choose the privacy information they are willing to be processed by the platform one by one.

3) The principle of informed consent is not directly applicable to all types of privacy provisions. For the service or commodity platform specifically for special groups, such as education services for minors, elderly care services and auxiliary services for the disabled, more humanized "informed" and "consented" methods should be adopted to better protect the privacy rights of special groups. For consumers with special groups who have the capacity for civil conduct to understand the privacy terms, the platform

ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

should fully assist them to understand the privacy policy content, while for consumers who cannot fully understand the privacy terms, the platform should prudently decide the service method and the processing process of private information, and if necessary, it can adopt flexible methods such as "consent" entrusted by the consumer.

5.1.2. The scope of "inclined protection"

The fundamental starting point of law is to balance the allocation of rights and obligations and reasonably adjust various interest relations. In the case of recognizing the inequality brought by the difference of status, inclined protection advocates taking special measures to give special protection to the disadvantaged. The emergence and development of the theory of inclined allocation of rights is to correct the defects caused by the one-sided emphasis on the principle of formal equality in the liberal concept, which reflects the concept of right protection from formal equality to substantive equality. [13]The concern for the individual is also the legislative spirit of China's civil code, consumer rights and interests protection law and other rules, just as Montesquieu stressed in the Spirit of Law: "In the motherly eyes of civil law, each person is the whole country". [14]However, if slanting protection does not set reasonable limits, it will overcorrect and fail to realize substantive equality. Therefore, it is crucial to pay attention to its scope limits. The diversification of interest subjects of online consumer privacy data rights determines that the protection of data rights subjects, relevant interest subjects, market order, the public and other interests should be considered comprehensively. [15]Considering the transaction security and efficiency comprehensively, the category of "privacy" should be reasonably determined for the legislative and judicial inclined protection of online consumers' privacy rights. in its 2012 report "ProtectingConsumer Privacy in an Era of Rapid Change", the US Federal Trade Commission said: Recom-mendations for business and policymaker classifies consumers' personal information according to consumer sensitive personal information and general personal information. Based on this, the required forms of consumer consent for different types of information are divided into three levels. In the case of setting the bottom line clause for the category of private information to adopt legal principles, detailed provisions for online consumption of the category of privacy and according to the sensitivity of information to distinguish, to achieve hierarchical accurate management. Correctly define the concept of rational use of private information by e-commerce platforms and other subjects, support platforms to accelerate the flow and dissemination of information data on the basis of clear sharing paths, so that online consumer privacy information can also participate in the big data economy track, and achieve positive interaction between consumers, platforms and third party data users. Promote the sharing and free use of data without infringing on the rights of data subjects and obtaining the authorization of data subjects. Overall protection of online consumer privacy and healthy development of platform economy.

5.2. Strengthen the principle of fiduciary duty

Fiduciary duty is an important legal system to solve the problem of lack of trust in digital society. It is closely related to social trust in specific fields and aims to prevent the risk of infringement in personal information processing by filling obligations. [16] When consumers choose to trust the promises of the platform in the privacy clause and continue to trust in the subsequent actual use process, online consumers have fiduciary interests, and the platform and other privacy protection subjects thus generate fiduciary obligations, and "breaking the promise is abuse of this trust".[17]

5.2.1. Expansion from the investment and financing field to the whole field

At present, the discussion of "fiduciary duty" in Chinese academic and practical fields is more focused on the field of investment and financing. However, we should realize the interest characteristics of online consumer privacy information and privacy rights themselves, which are inherently exchangable, fluid and tradable. We should ignore the dual economic significance of personal data for consumers and platform economy in the era of online consumption. It is not advisable to exclude privacy from the scope covered by "fiduciary duty". In fact, the dissemination of consumer privacy is more frequent in the era of platform economy than in the past. After privacy flows out of the data producer, it is no longer under the direct control and possession of consumers. The power of consumers for their own privacy is limited to the right to delete, cancel and other postrights. From this point of view, its "fiduciary interest" is more like a kind of natural rights rather than created interests, and its fluidity enables it to have multiple obligatory subjects.

5.2.2. Implement multi-subject responsibilities

At present, online consumer privacy protection has been expanded from the traditional single-line structure of consumer - merchant to the multi-party structure of consumer - merchant - platform -

ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

government - third-party evaluation agencies. Both the realization of consumers' right to obtain information and the protection of consumers' right to personal information, operators are the most important subject of obligation. [18]The state has the obligation to establish an effective system of government supervision and administrative law enforcement in advance to effectively prevent the occurrence of damage in order to protect the rights of citizens. [19]The function of the responsibility subject is more inclined to the question of who should take the initiative. At present, there is no lack of academic circles incorporating the evaluation system and prior supervision into the legal liability investigation system, so as to better play the role of the government and other competent departments and even the third-party evaluation agencies in protecting consumers' privacy rights online.

5.3. Introduce the third-party evaluation system of consumers' privacy

Extraterritorial experience -- Based on Sur-veillance Impact Assessment.The EU established this system earlier, originating from Prior Checking under earlier data protection regimes, followed by the introduction of Sur-veillance Impact Assessment by scholars, Which identifies, assesses and addresses risks to the regulatory system through consultation with stakeholders. (David Wright and Charles D. Raab, 2012). In addition, the California Consumer Privacy Act (CCPA) provides that the California Attorney General is responsible for the enforcement of the Act in accordance with relevant provisions, and for companies that violate their obligations by not implementing and maintaining reasonable security procedures to protect unencrypted or unedited personal information (Stuart L. Pardau,2018). Also in the European Union, the General Data Protection Regulation promulgated in 2018 was formulated in response to many cases of information and privacy data leakage in Europe. The regulation specifies that companies need to create data protection officers (Dpos) (similar to CEO and COO executive positions) responsible for personal data protection. By referring to the third-party evaluation mechanism of consumers' privacy rights and combining with the actual development of e-commerce platforms in our country, it is imperative to establish a set of evaluation system that conforms to the national conditions.

6. Conclusions

Through the empirical analysis and theoretical review, we know that the privacy clauses negotiation mechanism of e-commerce platform is short, the information sharing rules are fuzzy, and the main protection function failure is prominent. As a medium through which consumers transfer part of their rights and e-commerce platforms obtain part of their information rights, privacy clauses are not only related to whether platforms can normally analyze consumer behaviors through big data and make correct business decisions, but also whether online consumers' privacy rights can be guaranteed. In view of the current practice, the privacy clauses of e-commerce platforms are more serious in the form of formality, and they neglect to protect the privacy of consumers in terms of form and content. As a result of the threshold of reading the privacy clauses, few consumers have a real careful review, and the right to "inform -- agree" has not been substantially implemented. Slanting protection is in urgent need of strengthening. In the process of consumers using e-commerce platforms, a large amount of privacy information is not shared in a transparent and open channel, and consumers cannot be informed of the flow of information in a timely manner. The failure of subject responsibility leads to the absence of regulation. A long-term and flexible regulatory mechanism needs to emphasize the fiduciary duty of participants, but also requires the joint participation of e-commerce platform, government and third-party evaluation platform. Based on national conditions and learning from experience outside the region, a scientific and reasonable evaluation mechanism is gradually established to provide conditions for the reactivation of subject responsibility and supervision.

References

[1] He Peiyu, Wang Xiaorui. Research on the Privacy Security Mechanism of Smartphone users -- Based on the analysis of the "Privacy Clauses" of third-party applications [J]. Information Studies: Theory & Practice,2018,41(10):40-46.

[2] Liu Chunquan. Nature and Legal Liability of E-commerce Platform [J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition),2016,28(04):61-66.

[3] Liu Bailing, Wan Lulu, Li Yanhui. A Review of Privacy Protection Based on Privacy Policy in the Network Environment[J] .Information Theory & Practice, 2016,39 (9): 134-139.

[4] Zhang Yuan, Zhu Xiaoyan. New Contract in the Internet Era, Network Format Contract[J]. Contemporary Law Review,2002(12):55-58.

ISSN 2616-7433 Vol. 5, Issue 8: 122-133, DOI: 10.25236/FSST.2023.050816

[5] Yi Bin, Liu Ying,Fang Jinping,Jia Songlin.Investigation and Reflection on the Privacy Policy of electronic resource supplier Website [J]. Library,2013(05):52-54.
[6] Lv Bingxin. On the Characteristics and Regulation of Network Standard Contract Clauses [J]. Law Science Magazine,2022,43(03):132-148.
[7] Chen Shiyang, Liu Tingting. Esearch on privacy policy issues and countermeasures of short video applications [J]. Information and Communications Technology and Policy,2020(02):74-77.
[8] Liang Dong. Standardized path of E-commerce consumers' personal information protection: An empirical study based on 6 categories and 12 e-commerce platforms' privacy Policies [J]. Journal of Dalian University of Technology (Social Science Edition),2022,43(03):102-112.
[9] Qi Aimin. Original Theory of Information Law, Wuhan University Press, 2010, 76.
[10] John Locke, translated by Zhao Boying et al. Two Treatises of Civil Government [M]. Shaanxi People's Publishing House, 2004.
[11] Zhang Xinbao. Collection of Personal Information: Inform the Restrictions on the Application of the Consent Principle. [J]. Research on Comparative Law,2019(06):1-20.
[12] Yan Kunru. Big Data Sharing-Privacy Paradox[J]. Journal of Dalian University of Technology (Social Science Edition),2020,41(05):15-20.
[13] Ji Nianfang, Ji Jinhua. The Allocation of right Inclination and its Limit: A Case Study of dismissal protection System [J]. Journal of PLA Nanjing Institute of Politics,2011,27(04):54-57.
[14] Montesquieu, Translated by Xu Minglong. The Spirit of the Laws [M], The Commercial Press,2012.
[15] Zhou Linbin. Legislative Ideas for the Allocation of Data Rights[J]. People's Tribune,2021(15):82-84.
[16] Xiang Qin. On "Weakening" of Personal Consent and "Supplementing" of fiduciary Duty in Personal Information Processing [J]. Journal of Law Application,2022(11):58-68.
[17] Anthony J. Bellia Jr., Promises, Trust, and Contract Law [J]. American Journal of Jurisprudence, 2002(47):25-40.
[18] Zhang Shouwen. Legal Development and Comprehensive Protection of Consumer Information Right [J]. Law, 2021(12).149-161.
[19] Zhou Hanhua. Legal Orientation of Personal Information Protection [J]. Studies in Law and Business, 2020,37(03).71-73.