CSCanada
Higher Education of Social Science
Volume 26, Number 1, 2024, pp. 39-47
DOI:10.3968/13333

ISSN 1927-0232 [Print]
ISSN 1927-0240 [Online]
www.cscanada.net
www.cscanada.org

Review and Path Optimization of the Application of "Informed Consent" Rules in Personal Data Protection

CHEN Siyu[a],*; BAI Fengming[b]

[a] Lishui Open University,Law School of Jiangxi University of Technology, China.
[b] People's Court of Liandu District, Lishui City, China.
*Corresponding author.

Received 3 January 2024; accepted 14 March 2024
Published online 26 March 2024

Abstract

The institutional design of the individual-centered "informed consent" rules ignores the standardization requirements for data processing at the social level. The neglect of data processors leads to vague regulations on their behavioral guidelines, the data processors are evasive in terms of notification content, and present the form of information in an impersonal way. Also, digital technology has become a convenient tool for evading or even violating the law, which will create obstacles to the application of rules and may even deviate from the original intention of legislation. In the application process of the "informed consent" rules, data processors should first respect the individual, provide sufficient and accurate notification and ensure the validity of the data subject's consent. Individuals should pay attention to their important role in the implementation of the law and promote the implementation of the "informed consent" rule. In addition, differentiation and application of opt-in and opt-out mechanisms, as well as a correct understanding of exceptions to the "informed consent" rule will help balance the relationship between individual data protection and the social processing of data.

Key words: Personal data protection; Informed consent; Data processing

Chen, S. Y., & Bai, F. M. (2024). Review and Path Optimization of the Application of "Informed Consent" Rules in Personal Data Protection. *Higher Education of Social Science*, *26*(1), 39-47. Available from: URL: http://www.cscanada.net/index.php/hess/article/view/13333
DOI: http://dx.doi.org/10.3968/13333

1. INTRODUCTION

In 2012, the Standing Committee of the National People's Congress proposed for the first time in the "Decision on Strengthening Network Information Protection" that data collectors should clearly state the purpose, method and scope of collecting and using information, and obtain the consent of the data subject. The 2013 "Credit Information Industry Management Regulations" made specific provisions on the "informed consent" rules, regulating credit reporting agencies in terms of emphasizing written consent and effective notification, becoming the first administrative regulation to implement the informed consent rules. The "Guidelines for the Protection of Personal Information in Information Security Technology, Public and Commercial Service Information Systems" implemented in 2013 set national standards and regulations for the protection of personal data in my country for the first time. It integrated the "informed consent" rule into all information processing links and stipulated A distinction is made between the forms of consent. Subsequently, the "Regulations on the Protection of Personal Information of Telecom and Internet Users" and the "Regulations of the People's Republic of China" were promulgated one after another.

Normative legal documents and non-normative documents such as the "Consumer Rights Protection Law" and the "Information Security Technology Personal Information Protection Guidelines" have strengthened and refined the "informed consent" rules from different angles and different scenarios. Based on the legislative experience of personal data protection in the Cybersecurity Law and the Civil Code, the Personal Information Protection Law basically establishes a legal protection framework for personal data with the "informed consent" rule as the basis and core. System, the future supplement and improvement of the legal system for personal data protection and processing will also be based on the "informed consent" rule.

2. QUESTION RAISING

"Informed consent" rules originated in the 1970s. At that time, the role of the Internet was still limited to the release and transmission of data, and e-commerce applications had not yet really appeared. Therefore, the creation of "informed consent" rules was still based on simple computer automation. In the context of processing personal data. However, after half a century, digital technology has matured and is still developing rapidly. Internet commerce has become ubiquitous. The advent of the big data era has made personal data more open and global, and the scale of data processing has increased accordingly. Data mining and analysis technologies allow the value contained in large-scale personal data to be exploited, and the value of data flow is increasingly emphasized. At this point, the legitimacy of the "informed consent" rule is questioned: Is it still necessary to continue to allow data subjects to maintain control of their personal data? Can the data subject's right to informed consent be effectively exercised and the standardization of data processing ensured? This triggered intense debate in academic circles at home and abroad. The "informed consent" rule was born in the era of small data. Its purpose is to safeguard individual autonomy and dignity. At the same time, the obstacles to its application have not yet appeared. With the development of digital technology, the inherent information asymmetry between data subjects and data processors has been infinitely amplified, which has naturally challenged the application of "informed consent" rules. The gap seriously hinders the application and implementation of the "informed consent" rule. The overload, obscurity and professionalism of the data processor's "notification" content seriously hinders the data subject's understanding of the personal data protection policy, and the lack of effective content greatly reduces the exercise of the data subject's right to know. Data processors formally fulfill the legal obligation to "notify", but in essence they use this to respond to legal supervision and thus escape from legal obligations and responsibilities. Big data technology has seriously hindered the risk-dispersing function of the "informed consent" rule. The personal data protection system established in my country's "Personal Information Protection Law" still centers on the "informed consent" rule. Whether this rule can be accurately interpreted and structured not only determines whether the "Personal Information Protection Law" can be implemented, but also determines whether the "Personal Information Protection Law" can be implemented. It also determines whether the Personal Information Protection Law can achieve its dual mission of protecting personal data and promoting the orderly flow of data. Therefore, it is necessary to conduct a comprehensive review of the past application of the "informed consent" rule and provide a doctrinal explanation for its future application.

3. DIFFICULTIES IN THE IMPLEMENTATION OF "INFORMED CONSENT" RULES REVEALED

3.1 Inherent dilemma in the application of "informed consent" rules - information asymmetry

The theory of information asymmetry points out that in market economic activities, the parties have different understandings of relevant information. The party with more information will occupy an advantageous position in transaction negotiations. Information known only to one party is private information. Usually, The existence of private information is the motivation for the party with abundant information to start a transaction, and sometimes even determines the outcome of transactions and negotiations.This kind of information asymmetry will affect the conduct of fair transactions and have an impact on the rules of autonomy of will. The lemon market theory believes that information asymmetry will lead to the phenomenon of "bad money driving out good money", causing the market to shrink or even disappear. From an efficiency perspective, information asymmetry will aggravate market failure, generate information economic rent, reduce the probability of successful transactions and even lead to transaction failure. In fact, with the deepening of social division of labor, information asymmetry is prevalent in various social relationships, such as between consumers and operators, employers and employees, patients and doctors, clients and lawyers, etc. In a principal-agent relationship, each party has knowledge and information advantages over the other party. However, in the relationship between data subjects and data processors, this asymmetric effect has been further intensified, the vicious market impact of information asymmetry has also expanded, and the relationship between the two has deteriorated sharply.

Regarding the data processing process, its value and the risks that may arise therefrom, the data processor has a very obvious information advantage compared to the data subject. However, due to the limitations of professional and technical knowledge, this technical process is almost a "black box" for individuals. In a society where smart terminal devices and mobile Internet are ubiquitous, data subjects may not even know whether personal data is collected. For example, facial recognition technology is concealed, and consent is impossible to discuss. Secondly, individuals do not know whether the data processor's use of big data technology to process personal data can further deduce or analyze potential and additional personal data or even sensitive data, which may exceed the consent of the data subject. range or expectations. Third, data processors can take advantage of this asymmetric position to spread risks and use technological advantages to strengthen data subjects' dependence on them, thereby

suppressing the exercise of the right to informed consent, because individuals often need the technology possessed by data processors to enjoy their lives. convenient. Finally, due to the internal or even secretive and professional nature of data processing, data subjects cannot determine or prove whether the actions of the data processor violate their legitimate rights and interests. Therefore, the key difference between a data processing relationship and other asymmetric relationships is whether the harm or harm is identifiable. In a traditional asymmetric relationship, if the rights and interests of the party with information disadvantage are violated, the injured party can directly feel it, such as directly suffering material damage to property or body, or mental damage such as reduced social evaluation. However, when the data processor performs data processing beyond the scope of the data subject's consent or expectation, the individual will not suffer direct material or mental damage. Even if he suffers a certain degree of mental damage, the existence of the infringement result or even the illegal behavior and the result are proved. The relationship will also be a difficult problem that needs to be solved for individual rights protection.

In addition, although the results of the data processor's infringement on the rights and interests of the data subject are concealed and indiscernible, from the perspective of the long-term data processing process, the accumulation and continuation of such infringement may lead to the damage to downstream individuals. It broke out during the process of data processing, but at this time it was too late to provide relief to the data subject, which resulted in the institutional prevention and deterrence functions of the "informed consent" rule being unable to function.

3.2 The falsification of "notification" and its denial of the right to informed consent

3.2.1 Overload of informed content and insufficient information

The completeness, clarity, and understandability of matters such as personal data collection, use, sharing, and user rights in the personal data protection policy will greatly affect the data subject's willingness and emotion to read, and thus affect his or her decision to process personal data. Understand and be informed. However, many companies seek to legitimize and legalize data processing and avoid liability, making personal data protection policies a mere decoration. From a formal point of view, the personal data protection policies of many software and websites have lengthy terms, and the privacy policies of many mainstream websites are more than 10,000 words long. This greatly increases the user's reading burden and reduces their willingness to read, and even causes information overload and affects the user's information processing. In addition, personal data protection policies are also filled with a large number of professional terms and knowledge in privacy protection, technology and law. Only a few privacy policies provide key summaries and explain and explain professional terms, nouns or expressions. Note, this poses a great challenge to the reading ability of ordinary users. Some studies even believe that today's personal data protection policies are formulated by professional legal and privacy protection experts and have never been tailored for users. , its purpose is not to facilitate individual users' understanding and knowledge. Judging from the professionalism of the content, only lawyers and other experts with professional legal and technical knowledge can understand the information contained therein.

Judging from the long and lengthy personal data protection policy mentioned above, it is generally reasonable to believe that this is the good intention of the data processor. Its purpose is to prevent the leakage of everything, and to provide as much detail as possible on the key points of personal data processing and its possible risks. Inform, illustrate and explain. But unfortunately, the formal sloppiness conceals the lack of effective information transmission in substance.

First of all, during the initial collection of personal data, most companies or websites do not separately monitor the collection of personal data.

Notify the types of personal data and their corresponding purposes, Even if the relevant purposes are notified, but such as "providing better products and services", "improving the accuracy of services" and "providing a better experience" , "meeting needs" and other expressions are too vague and do not have a relatively certain connotation. There are also unclear explanations on the types of personal data collected and whether and how to use data collection tools and technologies such as cookies and beacons to collect personal data. This conceals the data processor's true motivation for collecting personal data, which is precisely what the data subject is most concerned about.

Secondly, in terms of the use of personal data, the description of the use of data is not very optimistic. It is not clear that personal data can be processed without consent. On the issue of whether the data processor needs to obtain consent again for use beyond the scope of consent or authorization. Ambiguity increases the potential for data processors to misuse personal data.

Thirdly, in terms of the sharing and transfer of personal data, in practice most websites may provide personal data to the outside world. However, most websites have vague definitions of data recipients such as data, affiliates, third parties, etc., and such terms as "rich third-party services" and "Expressions such as "protecting affiliated companies" and "recommended information" make the situation and scope of personal data transfer almost unlimited, which essentially conceals the illegal trading of data.

Again, in terms of personal data security protection, only a few websites mention the security risks that may arise after users provide personal data. The security

protection of personal data mainly includes security technical measures and security management measures and responses, including personal data storage, deletion and exit, formulation of emergency plans, team or department settings, security certification and authority control, personal data protection policy The disclosure situation in this regard is also not ideal. In addition, most personal data protection policies will inform users of their rights, but lack specific operating mechanisms and ways to exercise rights. Data subjects also lack specific ways to correct personal data and withdraw consent. Users do not use the service or The exit mechanism for the product is also unclear. However, in the data processor's statement of responsibilities corresponding to the user's rights, the exemption is explained in detail, but the relevant personal data protection and legal obligations that it should bear are unclear, and there is even a violation of the personal data protection policy. Legal liability is agreed upon. In addition, personal data protection policies for minors are basically absent.

Finally, statements such as "The website reserves the right to temporarily or permanently update or modify (any part of) the privacy policy or terms at any time in the future, and will no longer proactively remind users/no further notice" are blatant violations of legal provisions and Disregard of the data subject's right to informed consent. In addition, the lack of marking of feedback channels and paths on the website reflects the data processor's indifference to the performance and compliance of notification obligations.

3.2.2 Chaotic and complex dehumanized forms of notification

Just as text content affects an individual's reading experience, the presentation form of personal data protection policies can also enhance or inhibit perceived effectiveness to a certain extent. Studies have shown that the form of personal data protection policy has a great impact on users' willingness to provide personal data and their intention to accept or purchase services or products. For example, when the personal data protection policy is in the default form and presented automatically, users are more inclined to actively spend energy and time reading it, and when the personal data protection policy requires more operations or steps to open, Individuals are more likely to skip the informed stage directly. However, in practice, data processors can easily use technical means and measures to set misleading, erroneous or even invalid links on relevant interfaces and screens, insert complex and difficult to understand tables and invalid keys, and even deliberately set up Pop-ups and advertisements with irrelevant content are used to block relevant content, which may interfere with the data subject's browsing of important matters such as personal data protection clauses, warnings and reminders, and consent, greatly reducing the effectiveness of the exercise of the individual's right to informed consent.

First, personal data protection policies or terms in practice are often named "privacy policies". However, the personal data protection policies of websites or companies in my country have different names and are relatively confusing, which can easily lead to individual cognitive biases and even mislead individuals' knowledge. For example, some are called "Privacy Policy" and "Privacy Statement", others are called "Privacy Protection Guidelines", "Information Protection Policy", "Privacy Protection Agreement", etc., and some even use other names, such as "License Agreement" ", "User Information", "Service Agreement", "Legal Statement", "Terms", etc. This is different from the situation where the personal data protection policies of most websites in the United States are basically uniformly named "Privacy policy" and "Privacy statement" and are displayed to consumers as separate parts. Although the data processor displays substantive personal data protection policies and clauses, the variety of titles can't help but make the data subject question: Are the contents of these policies, statements and clauses roughly the same? Will the difference in naming lead to differences in legal nature? Will they all be legally binding? This will undoubtedly cause unnecessary trouble to the data subject, causing them to question the notification and have doubts about the consent given, thus causing defects in the consent.

Secondly, the lack of words and titles such as "Privacy Protection" and "Personal Information Protection" and the inclusion of personal data protection clauses in user or service agreements only increase the burden on users to search and determine information, hiding valid and critical information. In the large amount of information, it may even cause users to give up their attempts to understand the personal data protection provisions. Such perfunctory notification can be regarded as a disguised refusal to inform, which also shows that the sincerity of the company in personal data protection is questionable.

Thirdly, as mentioned above, if the links and steps for individuals to query personal data protection policies can be reduced, it will increase their willingness to read personal data protection policies. An independent personal data protection policy can be directly displayed on the homepage of a website or software. It can serve as an effective reminder or even warning. However, there are situations where users are required to click links multiple times, and some websites and applications even require users to register before they can view the personal data protection policy. This means that individual consent is given before notification, which obviously infringes on data. The subject's right to know also renders the giving of consent meaningless.

Finally, any policy text that wants to convey effective information or attract readers should have a table of contents, abstract, title and classification, notes, topic sentences, central sentences and key points or key parts

at a macro level, and should be clearly layered and progressive. The key points are highlighted. On a micro level, fonts, font sizes, line spacing and even person names all affect the user's visual experience. However, some personal data protection policies have too few subtitles, resulting in a confusing framework and unclear logical system. The general introduction and lack of annotations make the text plain and boring. The use of the third person invisibly increases the distance between users and users. distance.

3.3 The failure of "informed consent" rules to operate in a big data environment

In the pre-big data era, personal data processing had specific purposes, and the scenarios for personal data processing were single, small-scale, and non-cyclical. Due to the limitations of computers and information and communication technologies, personal data processing matters were basically limited. Predictions can be made, which creates a favorable external environment for the operation and application of the "informed consent" rules. However, with the maturity of technologies such as the Internet, Internet of Things, cloud computing, and artificial intelligence and the improvement of computing power, big data processing technology has gradually become normalized and universal. First of all, the entire process of data processing can be carried out through digital or even intelligent equipment, which creates technical conditions for the confidentiality of data processing. Data processors can completely process data without the data subject knowing it.

Secondly, the core function of big data is discovery and prediction, which breaks through the traditional logical thinking model of causal reasoning and instead explores the correlation between things. This has resulted in the purpose and environment of personal data processing no longer being single, and the application scenarios of personal data have also become dynamic, diversified and complex, thus making the basic matters of personal data processing and the risks that may arise prediction becomes more difficult. Objectively, this not only causes trouble for the performance of the data processor's notification obligation, but also poses a huge challenge to the understanding and ability of data subjects without professional knowledge to the personal data protection policy. The validity of their consent also poses a huge challenge. It's suspicious.

Finally, the data aggregation effect under big data technology has become increasingly obvious. Not all the objects processed by big data technology are personal data, but even if it is non-personal data, or even if the individual has never provided or shared personal data, big data can also use algorithms to integrate personal and non-personal data guesses in different databases. Even identifying specific subjects,thus creating the risk of the subject's rights and interests being infringed. In this case, the data processor does not appear to have formally violated the "informed consent" rule because it does not process the personal data of an identified or potentially identifiable data subject, but it is highly likely that it will exploit the personal data of the data subject. When a subject's personal data is commercially exploited or otherwise processed, the risks that arise are exactly what the "informed consent" rules are intended to prevent and disperse.

4. BASIC STANCE AND PATH OPTIMIZATION FOR THE APPLICATION OF "INFORMED CONSENT" RULES

4.1 Basic position: The opt-in mechanism and the opt-out mechanism should be applied separately

The core of the opt-in mechanism is that the data subject expresses consent based on free will, and the data processor obtains the legal basis for processing personal data. The operation of this mechanism is based on the assumption that "the individual does not wish to participate" and requires that the individual must take clear actions to indicate participation. The opt-out mechanism refers to when the data processor informs the data subject that its personal data will be processed in an appropriate manner and declares that if the other party does not take special measures, it is presumed to "consent" to the relevant use of personal data. In individual cases, the meaning of "consent" can also be inferred from the specific behavior of the information subject. Therefore, the opt-in mechanism obviously provides higher protection to the data subject's right to informed consent, and also places higher requirements on data processors to obtain consent and its certification. If the opt-in mechanism is used in the entire process of data processing, it will undoubtedly impose a great burden on the data processor, create certain obstacles to the flow of data, and reduce the efficiency of data utilization. Therefore, in order to coordinate the protection of personal data and the social use of data, the division of labor and coordination of the opt-in mechanism and the opt-out mechanism have become an important way for "informed consent" rules to promote mutual understanding and interaction between individuals and society.

According to the clear provisions on consent in Article 14 of the "Personal Information Protection Law", both the initial data collection stage and the subsequent data utilization stage should be carried out within the scope of the data subject's express consent. However, as mentioned above, the integration function of big data and the diversification of data application scenarios make it even impossible for data processors to know in advance or even predict the basic characteristics of all data processing objects, purposes, functions, functions, methods and

application values. As well as the possible risks, [20] it is impossible to absolutely inform them, and the scope of the data subject's consent or authorization cannot be absolutely framed. At this time, if the data processor is required to inform all changes in data processing-related matters and obtain explicit consent, it will be too harsh, and it will make the data subject overwhelmed and cause information fatigue, and will also hinder the social flow of data. The core measurement criterion that affects the data subject's sense of personal dignity and acceptance of data processing is the harm or risk that the data subject perceives or may perceive.

Therefore, the risk of data processing behavior can be initially divided into two categories: low risk and high risk based on the personal data processing impact assessment mechanism established in the "Personal Information Protection Law". The classification standard can refer to the object and nature of data processing. , purpose, method, background, scope and possible harm to the data subject and other factors shall be determined. For example, processing of sensitive personal data and children's personal data, systematic and comprehensive evaluation, profiling and prediction of subjects based on automated decision-making, large-scale processing of personal data and processing for the purpose of large-scale surveillance, cross-border transfer of personal data movements, processing involving human dignity, which may lead to social discrimination, identity theft or fraud and damage to reputation or any other significant economic or social harm to the data subject, deprivation of the rights of personal data as well as revealing racial origin, political opinions, religious beliefs and The behavior of health, sexual life, genetic data and other information should be classified as high-risk data processing behavior. On the basis of determining the data processing behavior as low risk level or high risk level, it will be dynamically disclosed and the opt-out mechanism or opt-in mechanism will be applied respectively.

Of course, the above-mentioned dichotomy is still somewhat rigid and abstract and has great openness. In the process of exploring the applicable situations of the opt-in mechanism and the opt-out mechanism in the future, it should continue to be refined and classified into categories, such as Through a series of law enforcement and judicial cases, we extracted the processing and application scenarios of personal data, society's privacy concepts, cultural traditions, values, data industry development, business and industry habits, the closeness of the relationship between the data subject and the data processor, and even the subject's identity. Reasonable expectations for data processing functions, methods, scope, purposes and risks are used as the standard for risk level classification. Risk levels can even be further divided into lower risk, general risk, significant risk, high risk, extremely dangerous and other categories. Quantify it to provide concrete guidance and reduce assessment and judgment costs. Under the guidance of the risk concept, when the purpose, method or object of subsequent data processing changes, it still maintains the objective logical coherence and compatibility with the initial consented data processing and the subjectively expected continuity and recognition. Without the unity of knowledge, the selection mechanism can still be applied.

To sum up, the differentiated application of the opt-in mechanism and the opt-out mechanism alleviates the dilemma of rigid application of "informed consent" rules across the board. It not only relieves data subjects' consent fatigue, but also encourages them to be more cautious and sensitive in making consent, improving the It improves the quality of consent, while reducing the burden on data processors to obtain consent, promoting the efficient use of data under the premise that data processing risks are controllable, and promoting the balance of data interests among private subjects and between private subjects and public society. .

4.2 Object optimization: clarify the relationship between consent and other legal grounds for data processing

Due to the diversity of data processing scenarios and social life and the balance of interests, Article 13 of the "Personal Information Protection Law" does not use consent as the only legal basis for data processing, but instead constructs a diversified legal basis for data processing. sexual basis. However, this does not mean that consent has a parallel relationship with other legal grounds for data processing. Due to the legislative expressions of "necessity" in items 2 to 4 and "reasonable scope" in items 5 and 6 of this article, combined with the proviso in paragraph 2, consent and other legal basis should be considered as principles and exceptions Therefore, the scope and circumstances of application of items 2 to 6 of this article should be strictly limited. Otherwise, exceptions may become a normalized basis for data processing, thereby overriding the "informed consent" rule, and ultimately making this article The normative purpose has been defeated.

Regarding the circumstances specified in the second paragraph, it cannot be considered that as long as the data processing is subject to contractual consultation before the conclusion of the contract, the application of the "informed consent" rule can be excluded. The scope of the relationship before the contract is legally established is very wide, the time span may be longer, and there may be many stages. If a simple initial contact situation - such as a simple personal consultation and understanding of information - can also be used as the basis for data processing, then in the contract In widely used market economic activities, data processors will be able to disregard the wishes of all data subjects and use this as the basis for almost all data processing activities. At the same time, consumers will also be extremely cautious when

contacting or the costs of trading, contract formation and performance will rise significantly. Therefore, only when the parties to the contract have entered into substantive negotiations, or when the data processor must process personal data without consent otherwise the conclusion or performance of the contract cannot be concluded, that is, only when the processing of personal data without consent becomes This provision shall only apply if it is a necessary condition for the conclusion and performance of a contract. It should be noted that the expressions of intention of each party during the formation and performance of the contract here should be true and flawless, that is, there is no legal or agreed situation where the contract is not established or invalid. If the contract is not established, invalid, or revoked under legal conditions, data processing without consent will be illegal from the beginning. At this time, the data processor may bear corresponding legal liability and immediately stop data processing. If it wants to further process the individual data, the consent of the data subject is required.

Regarding the circumstances specified in the third item, it cannot be considered that the data processor can process personal data without consent as long as it is fulfilling legal duties or obligations. Combined with Articles 18 and 33 of the Personal Information Protection Law, and Article 35, unless otherwise specified, shall only apply if obtaining consent would prevent the data processor from performing its legal duties or legal obligations or make it impossible to continue or complete the activity.

The fourth item is the product of the interest balance carried out by the legislative body. An individual's life and property rights are obviously more important than the data subject's right to informed consent. The "natural person" here also includes individuals other than the data subject. The focus and difficulty of applying this rule in the future is to accurately define the connotation of "emergency situations".

In item 5, the legislature gives priority protection to freedom of expression for public interest purposes.

The sixth item is also an effort to balance data protection and flow, but the personal data in this item should be in a state that has been legally disclosed. Disclosure means disclosure to unspecified subjects, and all unspecified subjects can learn about the personal data through legal channels. If the disclosure of personal data is caused by illegal reasons, such as infringement of the legitimate rights and interests of the data subject, data leakage of data processors, illegal disclosure, etc., this provision cannot be applied. The standard of reasonableness can be determined from multi-dimensional perspectives such as the purpose of processing, the scope of processing, the method of processing, the risks that may arise from the processing, and the impact on the data subject. It should be noted that the opt-out mechanism still has room to be applied in the circumstances stipulated in this item. If the data processing will have a significant impact on the data subject, the opt-in mechanism should be re-applied at this time.

Interpreting the exception system of the "informed consent" rule abstractly in advance will inevitably encounter inevitable limitations, and it is impossible to foresee all corresponding specific situations, such as "necessity", "emergency situations", and "reasonable scope". The meanings of concepts such as "and "public interest" cannot be static. Instead, their connotations need to be explained and concretized based on multiple factors such as specific data processing scenarios, historical and cultural traditions, and popular concepts of the public. Construct typed legal rules based on precedents. Therefore, how to properly handle the relationship between the "informed consent" rule and its exception rules, and then systematically and organically integrate the two into unified personal data processing rules, is the focus and difficulty of the future application of the "informed consent" rule.

4.3 Subject optimization: giving full play to the driving role of data subjects

Most personal data protection studies at home and abroad point the finger at data processors when criticizing and reviewing the effects of the application of "informed consent" rules. Most of them ignore the important position of data subjects in promoting the application of "informed consent" rules and even the progress of personal data protection governance. . Studies have shown that whether an individual's awareness and willingness to protect privacy and personal data is strong has a significant impact on whether to read the personal data protection policy and whether to make consent cautiously. [21] Therefore, the data subject's passivity bears unshirkable responsibility for the embarrassing dilemma encountered in the application of the "informed consent" rule. From the perspective of the above-mentioned relationship between individuals and society, society is shaped by countless individuals and their behaviors. Similarly, the implementation of "informed consent" rules also depends on the awareness and behavior of many data subjects regarding the management of personal data. Therefore, data subjects must take seriously the right to informed consent conferred by the law and actively safeguard it, otherwise, any improvement measures to the application of the "informed consent" rule will be of no avail.

Therefore, individuals should first choose operating systems and applications that have a higher level of personal data protection and respect users' right to informed consent, and browse or visit safe and compliant websites. They should take the necessary time to read and understand the personal data protection policy. If you read and If you lack understanding ability, you should strengthen your study of relevant personal data

protection knowledge and improve your own relevant accomplishments. Secondly, users should actively manage the personal data processing permissions of mobile applications and websites, avoid providing personal data at will and opening unnecessary personal data processing permissions, regularly screen, maintain, rationalize and update personal data, and monitor those who share personal data. Carefully weigh the benefits and risks, and decide whether to agree based on careful consideration. Finally, data subjects should actively exercise and safeguard statutory and agreed personal data rights and interests. When they find that personal data rights and interests have been improperly infringed, they should actively complain to data processors or industry associations or even seek public relief. This can also force data processing In order to respond to user and social pressure, enhance user trust and their own social reputation, and avoid legal penalties, they conscientiously implement the requirements of the "informed consent" rules and standardize data processing behaviors. The above-mentioned measures will certainly consume a lot of personal time and energy, but from a positive perspective, this should become a part of individuals' lives in the data society, because this is the data for individuals to enjoy the dividends of the development of the data era and bear the abuse of personal data. The price that must be paid for security risks is also the obligation that individuals in society should perform to control the risks of unlimited proliferation of data processing.

CONCLUSION

The practical experience of the rule of law at home and abroad at all times shows that absolutely perfect legal systems and rules do not exist. Any law or legal system is a product of the times or the result of multi-party social games. It is a manifestation of human limited rationality, so it inevitably has The limitations of the times and have a negative impact on the environmental system in which the rule of law operates. The key to China's "informed consent" rule system and its operating system is how to base it on the country's political and historical and cultural traditions while limiting possible disadvantages within the scope of what is acceptable to society or the public. The future interpretive and judicial system of "informed consent" rules will be constructed within the framework of the "Personal Information Protection Law" and combined with judicial and law enforcement practices, eventually forming a "law formulation" - "law implementation" - "society" A virtuous cycle of "feedback" - "law revision", "loophole filling" - "effectiveness" achieves symbiosis between individuals and society. The "Personal Information Protection Law", which is the basis for the construction of the "informed consent" rule system, has not been in effect for a long time, and reaching a consensus cannot be achieved overnight. In this regard, it is necessary to pay close attention to the trends in legal practice and promote the implementation of the "informed consent" rule in practice.

REFERENCES

Baek, Y. M., Kim, E., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior, 34*(2), 48-56.

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. *Communications of the ACM, 57*(11), 32.

Calo, M. R. (2012). Against notice skepticism in privacy (and elsewhere). *Notre Dame Law Review, 87*(3), 1027-1033.

Cao, D. (2019). *Research on my country's social media privacy policy text and personal information protection level*. (Master's thesis, China University of Political Science and Law).

Fan, H. Q., & Zeng, Z. (2016). Research on privacy policy statements of search engine companies: Taking Baidu and Google as examples. *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 4*, 58.

Feng, K. (2020). Inspection and reflection on the personal information 'opt-out' mechanism. *Global Law Review, 4.*

Huang, Q. (2014). *Research on the relationship between information asymmetry and market efficiency.* (Doctoral dissertation, Shandong University).

Lewis, S. D., Colvard, R. G., & Adams, C. N. (2008). A comparison of the readability of privacy statements of banks, credit counseling companies, and check cashing companies. *Journal of Organizational Culture, Communications and Conflict, 12,* 23-28.

Li, Y. (2014). On the protection of consumers' personal information: Focusing on consent after notification. *Theoretical Monthly, 8,* 124-128.

Li, Z. R., Tian, Y. C., Zhang, W. Z., & Liu, Y. (2020). Research on privacy policy of China mobile applications. *Cyberspace Security, 6*, 63.

Long, H. Y. (2019). *Research on personal information protection on my country's websites: Analysis of privacy policies based on 97 websites.* (Master's thesis, Chongqing University).

Maier-Schoenberg, V., & Cukier, K. (2013). *The era of big data: Big changes in life, work and thinking.* (Y. Y. Sheng & T. Zhou, Trans.). Zhejiang, China: Zhejiang People's Publishing House. (Original work published 2013).

Shao, G. S., Xue, F. W., Zheng, Y. Y., & Zheng, Y. (2018). Research on the personal information protection level of my country's websites: An empirical analysis of 500 websites in my country based on the "Network Security Law." *News Reporter, 3,* 63.

Steinfeld, N. (2016). I agree to the terms and conditions: (How) do users read privacy policy online? An eye-tracking

experiment. *Computers in Human Behavior, 55*, 992-1000.

Tan, Y. G., & Qian, X. P. (2006). Recommendations for improving the privacy protection policy of my country's websites. *Modern Intelligence, 1,* 216.

Weber, J. W. (2008). *The impact of e-commerce privacy policy statements on consumer willingness to disclose personal information.* Dissertations and Theses-Gradworks, 78-89.

Zhu, H., Zhang, M. G., & Lu, Y. H. (2018). An empirical study on social media users' intention to read privacy policies. *Journal of Information Science, 4,* 370.

Zhu, Y. (2017). Research on my country's mobile app privacy protection policy: Analysis based on 96 mobile application apps. *Journal of Jinan University (Philosophy and Social Sciences Edition), 12*, 111.