Practical Dilemmas and Improvement Paths of the "Separate Consent" Rule in Personal Information Processing

Jixuan Cui
School of Law, Xinjiang University of Finance and Economics, Urumqi, Xinjiang, China

Abstract: With the rapid development of the digital economy, the problems of excessive collection and misuse of personal information have become increasingly prominent. The Personal Information Protection Law of the People's Republic of China innovatively introduces the "separate consent" rule, aiming to remedy the shortcomings of the traditional "bundled consent" approach in specific sensitive scenarios and to strengthen the control rights of data subjects. However, in judicial practice and commercial applications, "separate consent" faces various practical dilemmas, including formalization, consent fatigue, ambiguous boundaries, and inequality of subject status. From an interdisciplinary perspective of civil law and data law, this paper analyzes the normative connotation of "separate consent," explores in depth the reasons for its ineffectiveness in practice, and proposes improvement paths. These include clarifying formal review standards, establishing a scenario-based application mechanism, introducing dynamic consent and withdrawal mechanisms, and strengthening the fiduciary duties of personal information processors. The aim is to restore the institutional vitality of the "separate consent" rule and achieve a dynamic balance between personal information protection and the circulation of data elements.

Keywords: Personal Information Protection Law; Separate Consent; Informed Consent; Scenario-based Theory

1. Introduction

In the era of big data and artificial intelligence, personal information has become a core driving force of the digital economy. However, as the value of data continues to be exploited, issues such as forced authorization by apps, excessive data collection, and covert data sharing—practices that infringe upon personal information rights—remain persistent despite repeated regulatory efforts. Article 1035 of the Civil Code of the People's Republic of China establishes the fundamental principle of "informed consent" in personal information processing [1]. Building upon this foundation, in order to address the risk of the erosion of data subjects' rights in complex data-processing scenarios, the Personal Information Protection Law of the People's Republic of China explicitly introduces the "separate consent" rule in several key provisions (such as the processing of sensitive personal information and the cross-border transfer of personal information).

"Separate consent" represents a breakthrough from the traditional model of "general consent" or "bundled consent." Its core objective is to ensure that, when faced with high-risk data processing activities, data subjects are able to exercise a more adequate, independent, and uncoerced right to make decisions. However, laws alone are insufficient to guarantee their own effectiveness. In commercial practice, due to the lack of a clear legal definition of what constitutes "separate" consent, coupled with the tension between profit-driven capital and users' cognitive limitations, "separate consent" is often reduced to lengthy privacy policy pop-ups or mandatory checkboxes, resulting in significant practical difficulties in its application. Therefore, clarifying the normative intent of "separate consent," confronting its practical dilemmas, and exploring pathways for its improvement are not only pressing theoretical issues in the field of civil law, but also practical necessities for regulating order in the digital marketplace.

2. The Normative Connotation and Institutional Value of the "Separate Consent" Rule

2.1 Normative Connotation and Legal

Characteristics of "Separate Consent"

"Separate consent" is not an institutional design that emerged out of nowhere. Although the EU's General Data Protection Regulation (GDPR) does not explicitly use the term "separate consent," it clearly requires that the data subject's consent be specific, informed, and unambiguous. Drawing on this framework and adapting it to domestic legal practice, China's Personal Information Protection Law transforms these requirements into the "separate consent" rule. Its core normative connotation can be summarized into two key dimensions:

At the formal level, such consent must be independent from general terms such as user agreements and standard privacy policies, and must be presented to individuals through dedicated forms, such as separate pop-up windows or standalone checkboxes.

At the substantive level, the data subject must grant authorization for a specific and singular purpose or act of personal information processing after careful consideration. Any form of bundled authorization or coerced consent is strictly prohibited.

According to the Personal Information Protection Law, "separate consent" is primarily required in five categories of high-risk personal information processing scenarios: providing personal information to third parties, publicly disclosing personal information, installing image collection devices in public places for purposes unrelated to public security, processing sensitive personal information, and transferring personal information abroad.

2.2 The Institutional Value of "Separate Consent": From Formal Autonomy to Substantive Autonomy

In the traditional civil law system, "consent" is a core manifestation of the principle of autonomy of will. However, in cyberspace, there exists a significant information asymmetry and disparity in bargaining power between information processors and individuals. The commonly adopted "bundled consent" model has often been reduced to a tool for platforms to evade responsibility, leaving autonomy of will merely at a formal level. The institutional value of "separate consent" lies precisely in breaking through this formalistic dilemma [2].

By imposing more stringent procedural requirements, it aims to awaken data subjects' awareness of the risks associated with high-risk processing activities, grant individuals the right to veto such activities, and thereby transform formal autonomy of will into substantive decision-making autonomy. In essence, it represents a concrete extension of the protection of personal dignity under civil law in the digital age.

3. Practical Dilemmas in the Application of the "Separate Consent" Rule

Although legislation has established an institutional framework of "separate consent" for personal information protection, in the complex ecosystem of the internet economy, the implementation of this rule is frequently hindered, and its intended protective function is significantly weakened.

3.1 Formal Distortion: The Proliferation of Dark Patterns and "Consent Fatigue"

In practice, many app operators exploit "dark patterns" in user interface and experience design to circumvent the substantive requirements of "separate consent." For instance, they may set consent checkboxes as pre-selected by default, design the "agree" button to be highly prominent, while hiding options such as "decline" or "not now" within multi-layered menus, or displaying them in extremely small fonts to reduce visibility.

An even more prominent issue is the phenomenon of "consent fatigue." Various apps frequently present users with repeated authorization requests; when opening applications or using new features, users are constantly confronted with lengthy legal texts and multiple confirmation pop-ups. Under conditions of bounded rationality, users often lose patience and mechanically click "agree" in order to access services quickly. In such circumstances, although the formal requirement of "separate" consent appears to be satisfied, the consent itself has already lost its substantive foundation of being informed and voluntary [3].

3.2 Ambiguous Boundaries: Overgeneralization in Defining Applicable Scenarios and Objects

Although the Personal Information Protection Law delineates five major scenarios for the application of "separate consent," in judicial

practice, there remain significant ambiguities regarding the boundaries of these scenarios and the identification of relevant objects. Taking sensitive personal information as an example, the law explicitly lists categories such as biometric data, medical and health information, and location tracking data. However, it remains unclear in practice whether data such as users' browsing histories or shopping preferences—once analyzed by algorithms—should also be classified as sensitive personal information, and there is no unified standard for such determinations [4].

In addition, in scenarios involving the provision of personal information to third parties, many platforms deliberately characterize their relationships with such parties as "joint processors" or "entrusted processors," rather than as instances of providing personal information to others. By doing so, they attempt to circumvent the mandatory requirement of "separate consent," resulting in the rule becoming nearly ineffective within the internal operations of large internet conglomerates [5].

3.3 Imbalance of Power: De Facto Coercion and Improper Bundling

The core prerequisite for valid consent in civil law is voluntariness. However, in the context of the digital economy, most major platforms possess quasi-infrastructural characteristics, placing users in a position of significant disadvantage. Although some apps formally provide options for "separate consent," they impose "take-it-or-leave-it" terms—users must either consent or cease using the service. If users refuse authorization, they may be unable to access core services or may experience a substantial degradation in service quality.

For example, in certain social media applications, if users refuse to separately authorize access to location data, they may not only be unable to use additional features such as "nearby users," but may also face restrictions on basic messaging functions. Such de facto coercive bundling turns "separate consent" into a tool that pressures users into compliance, thereby undermining its intended purpose and violating the fundamental principle under the Civil Code that prohibits the abuse of civil rights [6].

3.4 Difficulties in Judicial Relief: Challenges in Burden of Proof and Damage Identification

When users initiate civil litigation due to non-compliant "separate consent," they often face extremely high barriers to rights protection. On the one hand, there are significant difficulties in producing evidence: ordinary users find it hard to prove that they were misled at the time of giving consent, and are generally unable to demonstrate that their personal information was transferred or processed without obtaining proper separate consent.

On the other hand, it is difficult to identify and assess damages. Violations in personal information processing typically do not result in direct or tangible financial losses. The resulting infringements on personality rights and psychological distress, under the traditional tort liability framework of civil law, are unlikely to receive judicial support unless they reach the threshold of serious emotional harm. This situation ultimately leads to frequent inconsistencies in judicial decisions in similar cases [7].

4. Analysis of the Causes of the Practical Dilemmas in Applying the "Separate Consent" Rule

The difficulties in implementing the "separate consent" rule in practice stem, at a deeper level, from the conflict between legal logic and commercial logic. At the same time, traditional civil law theory also exhibits inherent limitations when addressing the unique characteristics of data as a production factor.

4.1 Profit-Driven Incentives under the Data Monetization Business Model

At present, the core of the internet business model lies in data monetization. Commercial activities such as targeted advertising and algorithm training all rely on massive, multi-dimensional personal data. Under this business logic, information processors are inherently motivated to maximize the collection of personal information [8].

However, "separate consent" essentially increases the transaction costs of data collection. In order to sustain the benefits derived from data, enterprises are likely to circumvent this rule through technological means, by exploiting regulatory grey areas, or by abusing exemptions such as the "legitimate interests" clause, thereby undermining its

effectiveness.

4.2 Inherent Deficiencies of the Traditional Informed Consent Model

In the practical context of personal information protection, even though the legal framework has introduced the seemingly more stringent mechanism of "separate consent," its essence still fails to transcend the theoretical framework and operational logic of the traditional "informed consent" paradigm. This classical model originated in the protection of patients' rights in the medical field, with the core objective of safeguarding individual autonomy through adequate disclosure of relevant information. Its theoretical premise consistently assumes that data subjects are fully rational economic actors, capable of comprehensively understanding highly specialized and complex information and making optimal decisions in their own best interests.

However, this assumption has encountered fundamental challenges in the digital age characterized by the widespread application of artificial intelligence and big data. Today, data processing chains continue to expand, cross-contextual reuse of data is increasingly frequent, and the "black box" nature of algorithmic operations renders their logic and rules highly opaque. Even legal professionals find it difficult to fully ascertain, within a short period of time, the potential scope of data authorization and the long-term privacy risks involved. Against this backdrop, it is clearly unrealistic to expect ordinary users, through a single act of "separate consent," to fully comprehend complex terms, anticipate unknown data risks, and effectively guard against privacy infringements. This demonstrates that merely strengthening "separate consent" is no longer sufficient to establish an effective safeguard for personal information protection in the digital era.

4.3 Insufficient Supply of Detailed Legislative Rules

China's Personal Information Protection Law is a framework-based and comprehensive piece of legislation, and it does not provide detailed implementing rules for "separate consent." For example, it remains unclear whether "separate" refers to an independent presentation in the user interface or to authorization granted at a distinct point in time. The law does not offer explicit operational guidance on this issue. The lack of detailed rules not only leaves broad room for interpretation by enterprises, but also increases the difficulty for regulatory authorities and judicial bodies in making determinations.

5. Paths for Improving the "Separate Consent" Rule

Addressing the practical dilemmas in applying "separate consent" cannot rely solely on the self-protection of data subjects, nor can it entail a complete rejection of the consent mechanism. Instead, it is necessary to take into account practical challenges and pursue comprehensive optimization across multiple dimensions, including formal standards, scope of application, technical mechanisms, and accountability systems.

5.1 Refining Formal Review Standards and Regulating Dark Pattern Designs

Legislation and regulation should establish more refined requirements for the formal elements of "separate consent," translating the principle of "substantive voluntariness" into concrete standards for interface design.

On the one hand, default pre-selection and manipulative design must be strictly prohibited. It should be clearly required that "separate consent" adopt an active opt-in mechanism. The "agree" and "decline" options should have equal visual prominence, and any use of dark patterns—such as color fading or hidden navigation paths to mislead users—must be strictly forbidden.

On the other hand, a simplified consent framework should be promoted. Drawing on the duty of notice for standard contract terms, information processors should be required to clearly inform users—within 100 words and in plain language—of the purpose of data processing and potential adverse consequences, using visual aids, layered presentation, and other accessible formats, so as to mitigate information asymmetry [9].

5.2 Introducing a Contextual Approach to Clarify the Scope of Application

"Separate consent" should not be applied in a rigid, one-size-fits-all manner; instead, it should be flexibly adapted through the lens of contextual privacy theory. Regulatory

authorities should promptly issue lists of core functions for different types of applications. For personal information necessary to provide core functions, general consent or exemptions based on contractual necessity may be applied; for ancillary functions and high-risk processing scenarios, however, "separate consent" must be strictly required, and refusal to grant such consent must not be used as grounds to restrict access to core services [10].

At the same time, a dynamic identification mechanism for sensitive personal information should be established. If ordinary personal information, when analyzed through algorithms in specific contexts, generates a high risk of harm—such as inferring sexual orientation or medical history—it should be treated as sensitive personal information and be subject to the "separate consent" requirement.

5.3 Establishing Dynamic Consent and Convenient Withdrawal Mechanisms

In response to the increasingly prominent issues of consent fatigue and the dynamic evolution of usage scenarios in practice, it is necessary to decisively abandon the traditional static and rigid approach of "one-time authorization with long-term validity," and instead establish a dynamic consent mechanism suited to the characteristics of the digital age.

Specifically, for separate consent involving the continuous collection of sensitive personal information—such as location data, contact lists, call records, and biometric data—a reasonable and strict validity period should be clearly defined. This would change the previous situation in which authorizations remained valid indefinitely after being granted, gradually fading from users' awareness. When platforms need to continuously access highly privacy-sensitive permissions, such as real-time location, or frequently activate microphones and cameras, they should not rely solely on a one-time authorization obtained during initial installation or first use. Instead, they should proactively, clearly, and without interference prompt users at regular intervals—such as every six months or other fixed periods—to reconfirm whether they wish to continue granting such authorization. This ensures that user consent is always based on their current and genuine intent, thereby safeguarding its contemporaneous validity and voluntariness.

At the same time, it is essential to strictly implement the core right, as established in the Personal Information Protection Law, for users to withdraw consent at any time, and to rectify the current unreasonable situation in which "authorization is easy, but withdrawal is difficult" on some platforms. At the legislative and regulatory levels, platforms should be explicitly required to design and provide a one-click withdrawal function that is as convenient as the authorization process itself. The withdrawal option must be prominently displayed in easily accessible locations, such as the app homepage or the main privacy settings page, ensuring that users can quickly exercise their rights without complicated navigation.

Furthermore, platforms must be strictly prohibited from imposing unreasonable obstacles, such as requiring users to mail written materials, complete lengthy application forms, upload photos holding identification documents, or wait for prolonged manual review processes. These cumbersome procedures, which effectively obstruct users from withdrawing consent, should be eliminated. Only by achieving procedural equivalence in convenience between authorization and withdrawal can consent fatigue be alleviated at the institutional level and the privacy risks arising from ever-evolving data collection scenarios be effectively addressed.

5.4 Strengthening Fiduciary Duties of Processors and External Oversight Mechanisms

Given the inherent disadvantaged position of individuals in the digital environment, it is difficult to fundamentally alter this imbalance. Therefore, external checks and balances must be introduced, shifting from a protection model that relies solely on user consent to one that emphasizes the statutory responsibilities of information processors. Drawing on the principles of trust law, fiduciary duties should be established for large data-processing platforms, requiring them to uphold duties of loyalty and care toward users. Even where separate consent has been obtained, if the processing activities violate legitimate and lawful purposes or cause substantial harm to users, platforms should still bear legal liability [11].

At the same time, judicial relief mechanisms

should be improved. In litigation involving infringements of "separate consent," the burden of proof should be reversed, requiring information processors to demonstrate that they have complied with the procedures for obtaining separate consent and that no bundling or deceptive practices have occurred. For platforms that systematically employ dark patterns to circumvent regulatory requirements, procuratorial authorities and consumer protection organizations should be empowered to initiate public interest litigation for personal information protection, thereby significantly increasing the cost of non-compliance for enterprises.

6. Conclusion

"Separate consent" is not only an important institutional innovation of the Personal Information Protection Law, but also a concrete extension of the principles of autonomy of will and the protection of personal dignity enshrined in the Civil Code in the digital age. In the face of issues such as formalistic compliance and disguised coercion driven by profit-seeking capital, the responsibility for personal information protection cannot be placed solely on the awareness and choices of ordinary users.

Only by refining formal review standards, clarifying the boundaries of contextual application, and establishing dynamic consent mechanisms—while fundamentally strengthening the fiduciary duties of information processors and enhancing objective legality review—can the current practical dilemmas be effectively addressed. In this way, "separate consent" can truly function as a rule-of-law safeguard against data abuse and achieve a balanced synergy between the development of the digital economy and the protection of personal information rights.

References

[1] Cheng Xiao. On Personal Consent in Personal Information Processing. Global Law Review, 2021, 43(06): 40–55.

[2] Lin Huanmin. On the Private Law Nature and Normative Application of Data Subject Consent—Also on the Non-uniformity of Consent in the Civil Code. Journal of Comparative Law, 2023, (03): 142–154.

[3] Wang Lizhi. Reflection on and Solutions to the "Informed Consent Dilemma" in Privacy Policies. Law and Social Development, 2023, 29(02): 210–224.

[4] Yang Weiqin. The Institutional Logic, Normative Interpretation, and Enhancement of the Informed Consent Rule for Sensitive Personal Information. Finance and Law, 2024, (01): 100–115.

[5] Chen Qian. On the "Contractual Necessity" Rule in Personal Information Processing. Administrative Law Review, 2023, (06): 134–145.

[6] Yang Xu. The Restricted Application of the "Contractual Necessity" Rule in Personal Information Processing. Legal Science, 2023, (06): 85–98.

[7] Fan Mingzhi. The Institutional Development of Public Interest Litigation for Personal Information Protection. Legal Science (Journal of Northwest University of Political Science and Law), 2025, 43(01): 109–121.

[8] Ma Gengxin. Improvement of the Personal Information Protection System in Data Transactions—Focusing on the "Informed Consent" Rule. Hebei Academic Journal, 2024, 44(02): 193–204.

[9] Guo Zhilong, Li Wenhui. The Application Dilemma and Breakthrough Approaches of the Informed Consent Principle in the Digital Age. Rule of Law Society, 2021, (01): 26–36.

[10] Liu Zhongxuan. Reasonable Limits of Personal Information Processing—A Contextual Analysis Based on the Principle of Necessity. Journal of Shanghai University of Political Science and Law (Rule of Law Forum), 2021, 36(05): 150–160.

[11] Feng Guo, Yan Haoyu. Theoretical Interpretation and Institutional Path of Fiduciary Duties of Data Trustees. Finance and Law, 2024, (02): 3–18.

