International Journal of Trend in Research and Development, Volume 13(5), ISSN: 2394-9333
www.ijtrd.com

Separate Consent in Facial Recognition: Application Dilemmas and Improvement Paths under PIPL Article 29

Yu Runze
Beijing Wuzi University, Beijing, China

Abstract: Facial recognition information, as a category of sensitive personal information, is subject under Article 29 of the Personal Information Protection Law of the People's Republic of China to the heightened requirement of separate consent. Nevertheless, the application of this rule encounters pronounced dilemmas in practice: the criteria for identifying separateness remain ambiguous; consent becomes increasingly formalized; static consent mechanisms are detached from the dynamic and cross-contextual realities of facial recognition technology; and principle-based legislation sits in tension with technologically complex scenarios. Drawing on contextual integrity theory, this article proposes several improvement pathways: clarifying the operational standards of separate consent in terms of interface independence, targeted disclosure, and express manifestation of consent; shifting from static consent to a dynamic consent mechanism featuring layered notice, continuous choice, and real-time updating; applying the rule in a differentiated manner according to specific contexts; and strengthening the coordinated safeguards of administrative supervision and judicial relief, including the presumption of fault and public interest litigation. Only through such a dynamic balance can the protection of facial recognition information and the rational utilization of technology be reconciled, so that every act of face scanning truly rests upon the autonomous, informed, and effective consent of the data subject.

Keywords: *Facial Recognition Information; Separate Consent; Sensitive Personal Information; Dynamic Consent; Contextual Integrity; Personal Information Protection Law*

I. INTRODUCTION

Facial recognition technology has become deeply embedded in virtually every corner of contemporary life. While the convenience it brings is remarkable, each act of face scanning entails, behind the surface, the collection and processing of the most sensitive category of biometric information. The human face is an innate biological feature of every person that can be neither altered nor replaced; once disclosed, it remains exposed to risk for a lifetime. For precisely this reason, the Personal Information Protection Law of the People's Republic of China (hereinafter the "Personal Information Protection Law" or "PIPL") expressly classifies facial recognition information as sensitive personal information and, in Article 29, subjects it to the more stringent consent requirement of separate consent.

However, a manifest tension exists between the strictness of legal regulation and the rapid iteration of technology. In the course of its application, the separate consent rule confronts a mechanical dilemma and proves unable to reconcile effectively the conflicting interests in the protection and utilization of facial recognition information. Scholars have observed that, although the PIPL imposes upon the processing of facial recognition information the requirements of separate consent and written consent, which are stricter than those applicable to ordinary personal information, the principled character of the statutory provisions still fails to alleviate the formalization of the informed consent principle in practice.[①] How to refine the application mechanism of the separate consent rule within the framework of the existing law, so that it can genuinely perform its institutional function, is a practical question demanding an urgent response.

Centered on Article 29 of the PIPL, this article focuses on the application of the separate consent rule in facial recognition scenarios. It seeks to analyze the causes underlying the rule's difficulty in being translated into practice and the institutional roots of its dilemmas, and accordingly attempts to propose corresponding pathways for improvement.

II. THE LEGAL ATTRIBUTES OF FACIAL RECOGNITION INFORMATION AND THE NEEDS FOR ITS PROTECTION

A. Conceptual Definition and Characteristic Analysis of Facial Recognition Information

Facial recognition information refers to the biometric data of the human face collected, stored, and analyzed through facial recognition technology, including facial geometry, facial texture features, and the feature templates generated through algorithmic processing. Unlike ordinary personal information such as names or telephone numbers, facial recognition information exhibits the following distinctive characteristics.

1. Direct Identifiability

The facial features of every individual are unique. Facial recognition information can directly pinpoint the identity of a specific natural person without being combined with any other information. This direct identifiability renders facial recognition information far superior to ordinary personal information in terms of identification efficiency.

2. Permanence and Immutability

A name can be changed, a password can be reset, and a telephone number can be replaced, but a face cannot be swapped. Once facial recognition information is leaked or misused, the data subject faces lifelong risk, and the danger cannot be eliminated by altering the information. This immutability means that, once facial recognition information is compromised, the data subject permanently loses control over it.

① 姜野.人脸识别技术应用的场景化法律规制[J].法制与社会发展,2023,29(1):208-224.

3. Non-contactness

Facial recognition technology can complete the collection of information without the data subject's slightest awareness. Compared with fingerprints, which require active pressing, or voiceprints, which require active vocalization, the collection of facial recognition information barely requires any active cooperation from the data subject, who may thus become the object of information collection without even knowing it.

4. Cross-contextual Penetrability

The human face is the most fundamental symbol of identification in social interaction, and facial recognition information possesses a natural capacity to penetrate across different contexts. Facial information collected by a processor in one context can be deployed for identification and analysis in another context. [②] Such cross-contextual fluidity substantially magnifies the risk of misuse.

B. The Normative Positioning of Facial Recognition Information as Sensitive Personal Information

In light of the above characteristics, the PIPL incorporates facial recognition information into the category of sensitive personal information. Article 28(1) of the Law provides: "Sensitive personal information refers to personal information that, once leaked or illegally used, may easily cause harm to the human dignity of a natural person or endanger his or her personal or property safety, including information on biometric identification, religious beliefs, specific identity, medical health, financial accounts, and whereabouts tracking, as well as the personal information of minors under the age of fourteen." As a paradigmatic form of biometric information, facial recognition information naturally falls within the scope of sensitive personal information.

The normative positioning of sensitive personal information entails that the processing of facial recognition information must comply with more stringent legal requirements. Under Article 28(2) of the PIPL, a personal information processor may process sensitive personal information only where it has a specific purpose and a sufficient necessity and adopts strict protective measures. This provision establishes the dual requirements of specific purpose plus sufficient necessity for the processing of sensitive personal information, thereby setting a high threshold of entry for the processing of facial recognition information.[③]

By differentiating among types of information, the PIPL has configured a strengthened regime of notice and consent for sensitive personal information. As the most special category within sensitive personal information, facial recognition information should naturally be subject to the strictest standard of protection.

C. The Distinctive Challenges in Protecting Facial Recognition Information

The particular attributes of facial recognition information give rise to distinctive challenges of protection that ordinary personal information does not face.

The first is the consent dilemma arising from technological asymmetry. Facial recognition technology is highly specialized, and data subjects often lack understanding of its basic principles, technical limitations, and potential risks; meanwhile, processors possess absolute discursive power over the interpretation of the technology. Such technological asymmetry makes it difficult to guarantee in practice the precondition of being fully informed.[④] The second is the risk of over-generalizing the public interest defense. Article 26 of the PIPL provides that the installation of image collection and personal identification equipment in public places must be necessary for the maintenance of public security and must be accompanied by prominent notice signs. In practice, however, the concept of public security risks being interpreted in an over-broad manner: commercial premises, office areas, and even school classrooms may all engage in information collection under the banner of security. The third is the irreversibility of the resulting harm. After ordinary personal information is leaked, the data subject can mitigate the damage by changing passwords or replacing accounts; but once facial recognition information is leaked, the data subject cannot change his or her face, and the resulting harm is permanent and irreparable.[⑤] This irreversibility requires the law to afford facial recognition information a higher standard of protection.

III. THE APPLICATION DILEMMAS OF THE SEPARATE CONSENT RULE

A. The Ambiguous Criteria for Identifying Separate Consent

The primary dilemma facing the separate consent rule is the ambiguity of the criteria for identifying what counts as separate. Although Article 29 of the PIPL imposes the requirement of separate consent, it does not define the specific meaning of separateness. In practice, some processors claim to satisfy the requirement by setting up a separate chapter in their privacy policies or by providing an independent check box. Yet it is doubtful whether such practices genuinely realize the separateness expected by the legislature, namely enabling the data subject to make an independent and focused decision on the processing of facial recognition information, free from interference by other consent matters. The mechanical application of the separate consent principle is also incompatible with the demand for convenience inherent in facial recognition technology.

The ambiguity of the identification criteria has produced multiple adverse effects. For enterprises, compliance standards are uncertain, making it difficult to formulate effective compliance schemes; for regulators, enforcement decisions lack clear criteria, making it difficult to unify the standard of enforcement; and for data subjects, it is impossible to judge whether their own consent truly satisfies the legal requirements, leaving the certainty of rights protection inadequate. In 2023, the Cyberspace Administration of China issued the Provisions on the Security Administration of the Application of Facial Recognition Technology (Trial) (Draft for Comments), which further regulates the processing of facial recognition information but still fails to provide sufficient detailed guidance on the operational standards of separate consent.

---

② 崔丽.个人生物识别信息的法律属性与保护路径——以《民法典》第 1034 条的解释为出发点[J].学习与探索,2021,(8):73-81.

③ 姜野.由静态到动态:人脸识别信息保护中的"同意"重构[J].河北法学,2022,40(8):126-144.DOI:10.16494/j.cnki.1002-3933.2022.08.008.

④ 杨惟钦.敏感个人信息告知同意规则的制度逻辑、规范解释与补强[J].财经法学,2024,(1):100-115.DOI:10.16823/j.cnki.10-1281/d.2024.01.007.

⑤ 丁晓东.隐私政策的多维解读:告知同意性质的反思与制度重构[J].现代法学,2023,45(1):34-48.

B. The Formalization of Consent

Even where processors formally satisfy the requirement of separateness, the quality of consent itself remains a problem at another level. In practice, consent to the processing of facial recognition information faces the same formalization dilemma as the general consent regime. Confronted with a pop-up window asking whether to consent, the data subject is typically faced with a binary choice of either consent or be unable to use the service. A separate consent given under such structural pressure, though formally separate, substantively lacks genuine voluntariness.

This model poses serious problems in practice. Operators' duty of disclosure becomes a mere formality, and the act of consent by data subjects lacks validity. Access to facial recognition is premised on the informed consent principle and the conditions for derogation from rights, yet both rules carry a risk of failure. Owing to the non-contact nature of facial information and the inherent power asymmetry between processors and data subjects, informed consent is difficult to implement.[6] Although separate consent adds a further procedural step in form, if that procedure still operates against the background of informational and power asymmetry, its institutional effect will inevitably be substantially discounted.

In addition, the hollowing-out of the right to withdraw consent is another prominent problem. Article 15 of the PIPL grants data subjects the right to withdraw consent, yet in practice data subjects often do not know how to withdraw consent, or find it difficult to exercise the right effectively even when they do. The right to withdraw consent thus faces the risk of being rendered nominal: the right is confirmed at the normative level but can hardly be effectively exercised at the practical level. For facial recognition information, which becomes irreversibly compromised once leaked, the ex post remedial value of consent withdrawal is inherently limited; if the right of withdrawal itself is also difficult to realize, the protection of data subjects becomes even more inadequate.

C. The Contextual Disjunction between Static Consent and Dynamic Technology

The deepest dilemma of the separate consent rule lies in the tension between its static institutional design and the dynamic reality of technology. The value of facial recognition information consists precisely in its capacity for repeated and cross-contextual use: facial information collected on one occasion may be deployed for multiple purposes. Yet the separate consent rule demands a one-off consent directed at a specific processing activity; once the data subject has given consent at the initial use, he or she is often unable to know how the information is subsequently reused or made to flow across contexts.

China's current protection of facial recognition information remains at the stage of static informed consent. Although rules on separate consent and consent withdrawal have been established, they can hardly reconcile the conflicting interests in the protection and utilization of facial recognition information, nor can they resolve the consent dilemma at its root.[7] A profound mismatch exists between the static separate consent rule and the dynamic application of facial recognition technology. Consent is given once at the starting point of information processing, but processing activities extend continuously over time, and the one-off consent given at the outset can hardly cover the subsequent, constantly evolving processing activities. Consent is directed at a specific processing purpose, but the purposes for which facial recognition information is utilized may change or expand during the course of processing. Consent is directed at processing within a specific context, but facial recognition information is inherently capable of flowing across contexts.

D. The Tension between Principle-based Legislation and Technologically Complex Scenarios

The three dilemmas described above are not isolated from one another; rather, they share a common institutional root.

Article 29 adopts a principle-based legislative model: it establishes the principle of separate consent but does not provide detailed rules on the concrete operational standards of separateness, the criteria for assessing the validity of consent, or the differentiated application of the rule across different scenarios. Scholars have observed, in commenting on the relevant provisions, that principle-based legislation, while preserving legal elasticity, also leaves considerable room for interpretation and uncertainty in application. Such principle-based legislation is not itself a defect, for it leaves room for the flexible application of the law; but when principle-based provisions confront a field in which technology iterates rapidly and application scenarios are complex, the problem of lacking detailed guidance is amplified.

As for the scenarios of application, the application scenarios of facial recognition technology are extremely diverse and expanding rapidly; the purposes, methods, and risk levels of information processing, as well as its impact on the rights and interests of data subjects, vary from one scenario to another. Scholars have pointed out that legal rules must be attuned to the scenarios of information processing, and that unified rules detached from specific contexts can hardly achieve precise governance.[8] The uniform application of a single standard of separate consent inevitably leads to the mechanical consequence of one size fits all: insufficient stringency in scenarios requiring strict control, and excessive rigidity in scenarios that do not. The current separate consent rule follows a command-and-control model of regulation: the law sets unified standards, enterprises passively comply, and supervision is backed by the threat of penalties. This model can still function effectively in a stable technological environment, but against the backdrop of the rapid iteration of facial recognition technology, legislation lags behind technological development, and reliance on this model alone can hardly achieve effective governance. Improving the separate consent rule requires simultaneous progress along multiple dimensions, including the refinement of rules, the transformation of the regulatory model, differentiated application, and the establishment of safeguarding mechanisms.

[6] 曾晨,李汶龙.人脸识别治理的进路完善:从个人信息到社会公正[J].学术交流,2024,(10):83-95.

[7] 林凌.人脸识别信息保护中的“告知同意”与“数据利用”规则[J].当代传播,2022,(1):108-112.

[8] 王锡锌.个人信息国家保护义务及展开[J].中国法学,2021,(1):145-166.DOI:10.14111/j.cnki.zgfx.2021.01.010.

IV. PATHWAYS FOR IMPROVING THE SEPARATE CONSENT RULE

A. Clarifying the Operational Standards of Separateness

First, the requirement of interface independence should be clarified. Separate consent should be independent, physically or functionally, from other consent matters. Specifically, processors should seek consent for the processing of facial recognition information through an independent pop-up window, an independent check box, or an independent signing page. Consent to the processing of facial recognition information must not be bundled with consent to the processing of ordinary personal information, with the signing of user agreements, or with any other matters into a single confirmation button. An independent interface enables the data subject to focus, free from interference by other matters, on the decision concerning the high-risk activity of processing facial recognition information. Interface independence is the most basic operational requirement of separateness.

Second, the requirement of targeted disclosure should be clarified. Before obtaining separate consent, processors should make a dedicated and focused disclosure specifically directed at the processing of facial recognition information. The content of the disclosure should include but not be limited to: the specific purpose and method of collecting facial information; the retention period; the manner in which facial feature templates are stored and the security measures adopted; whether the information will be provided to or shared with third parties; the rights enjoyed by the data subject; and the consequences of withholding consent. The disclosure should be presented in a prominent manner, in clear and comprehensible language, avoiding abstract and generalizing expressions. The requirement of targeted disclosure aims to ensure that, when giving separate consent, the data subject has obtained sufficient information directly relevant to the specific processing activity.

Third, the requirement of express consent should be clarified. Separate consent should be given expressly and may not be replaced by implication or presumption. Processors must not obtain consent through default selection or pre-ticked boxes, nor may they presume consent from the data subject's failure to respond. The manifestation of consent must be an affirmative and unambiguous act, for example, actively clicking the "Agree" button, voicing specific content indicating consent, or signing a written consent form. The requirement of expressness safeguards the certainty and provability of consent, which benefits both the protection of the data subject's rights and the processor's ability to demonstrate compliance.

B. Shifting from Static Consent to Dynamic Consent

Dynamic consent no longer treats consent as a one-off on-or-off switch action but understands it as a continuous and dynamic process of communication. It is necessary to introduce contextual integrity theory into the protection of facial recognition information, to apply a dynamic consent regime to the collection and utilization of facial recognition information, to configure opt-in and opt-out mechanisms dynamically, and to guarantee the data subject's right to be informed, thereby forming a dynamic consent model that accommodates the protection, circulation, and utilization of facial information.[9] Under the dynamic model, processors should offer data subjects opportunities to be informed and to make choices at every critical node of information processing: when facial information is collected for the first time, the data subject gives initial consent; when the purpose of processing changes, the data subject has the right to reassess and decide whether to continue consenting; and when the cross-contextual flow of the information may generate new risks, the data subject should be promptly informed and has the right to withdraw consent.

The institutional elements of dynamic consent are as follows. First, a layered notice mechanism: processors should inform data subjects in layers, according to the different stages and risk levels of information processing. Core information is disclosed at the initial stage, and supplementary notice is given at subsequent stages as the processing activity changes, rather than disclosing all possible content at once at the initial collection. Second, a continuous choice mechanism: data subjects have the right to make choices continuously throughout the entire course of information processing, including withdrawing consent after the initial consent, modifying the scope of consent, and giving new consent to new processing activities. Third, a real-time updating mechanism: when the purpose, method, or application scenario of processing facial recognition information undergoes a material change, processors should promptly update the notice to data subjects and obtain consent anew.

C. Differentiated Application according to Contexts

The standard of protection for personal information should not be uniform; rather, it should be determined according to the specific context in which the information is collected and used. Data subjects hold different reasonable expectations as to how their personal information will be processed in different contexts, and where a processor's conduct exceeds the reasonable expectations of the data subject, the consent given should be regarded as invalid or defective, even if it was formally granted. Introducing contextual theory into the application of the separate consent rule means that the assessment of the validity of separate consent should not remain at the formal level but should penetrate to the substantive level.

In the context of public security, the collection of facial recognition information is usually grounded in the statutory duty to maintain public security, and consent is not the sole basis of lawfulness. Article 26 of the PIPL has already imposed the condition of necessity for maintaining public security on the collection of facial recognition information in public-security contexts. In such contexts, the application of separate consent should appropriately yield to considerations of public interest, although processors remain subject to strict duties of disclosure and security assurance. In commercial contexts, the processing of facial recognition information is profit-oriented and admits no justification based on public interest; the separate consent rule should therefore be applied strictly, requiring processors to obtain the explicit consent of data subjects in an independent and prominent manner, and prohibiting the bundling of consent to the processing of facial recognition information with the provision of other services.

[9] 林凌.人脸识别信息保护中的"告知同意"与"数据利用"规则[J].当代传播,2022,(1):108-112.

Through differentiated application across contexts, the separate consent rule can achieve a precise match between the intensity of protection and the needs of each context, thereby avoiding a one-size-fits-all approach.

D. Strengthening the Coordinated Safeguards of Administrative Supervision and Judicial Relief

The national cyberspace administration and market regulation authorities should strengthen supervision and inspection of the processing of facial recognition information and impose penalties in accordance with law on conduct that violates the separate consent rule. Specifically, regulators should establish a supervisory system combining ex ante filing with ongoing and ex post supervision over the application of facial recognition technology. Ex ante filing requires processors, before commencing the processing of facial recognition information, to file with the regulators basic information such as the purpose of processing, the methods of processing, and the security measures adopted, so that regulators maintain a basic grasp of the processing activities within their jurisdictions. Ongoing and ex post supervision, through periodic inspections and the handling of complaints, continuously monitors processors' compliance and focuses on high-risk scenarios. At the same time, regulators should formulate and publish compliance guidelines for the processing of facial recognition information, providing processors with clear standards of conduct.[10]

Under Article 69 of the PIPL, where the processing of personal information infringes upon personal information rights and interests and causes damage, and the processor cannot prove that it is without fault, it shall bear tort liability including compensation for damages. In the application of the separate consent rule, where a processor fails to obtain the separate consent of the data subject in accordance with law, it should be presumed to be at fault and bear the corresponding tort liability. The presumption-of-fault rule substantially alleviates the burden of proof on data subjects and helps to enhance the practical effectiveness of the separate consent rule. Moreover, procuratorial organs may supervise and prosecute large-scale infringements of facial recognition information rights by instituting public interest litigation. Article 70 of the PIPL establishes the institutional basis for public interest litigation in personal information protection, providing an important procedural channel for the collective vindication of rights in respect of facial recognition information. Where large numbers of data subjects face the same or similar infringements, public interest litigation can effectively overcome the obstacles of high individual litigation costs and difficulty in proof, achieving the protection of rights at scale.

CONCLUSION

Facial recognition technology is reshaping social life at an unprecedented pace, and the separate consent rule embodies the legislature's special protection of human dignity in the digital age. Nevertheless, the tension between principle-based legislation and complex technological scenarios subjects the rule to manifold dilemmas. This article has sought to achieve a dynamic balance between strengthening the protection of facial recognition information and promoting the rational utilization of technology. Only in this way can every act of face scanning truly rest upon the autonomous, informed, and effective consent of the data subject.

References

[1] 姜野. 人脸识别技术应用的场景化法律规制[J]. 法制与社会发展, 2023, 29(1):208-224.
[2] 崔丽. 个人生物识别信息的法律属性与保护路径——以《民法典》第 1034 条的解释为出发点[J]. 学习与探索, 2021, (8):73-81.
[3] 姜野. 由静态到动态:人脸识别信息保护中的"同意"重构[J]. 河北法学, 2022, 40(8):126-144. DOI:10.16494/j.cnki.1002-3933.2022.08.008.
[4] 杨惟钦. 敏感个人信息告知同意规则的制度逻辑、规范解释与补强[J]. 财经法学, 2024, (1):100-115. DOI:10.16823/j.cnki.10-1281/d.2024.01.007.
[5] 晓东. 隐私政策的多维解读:告知同意性质的反思与制度重构[J]. 现代法学, 2023, 45(1):34-48.
[6] 曾晨, 李汶龙. 人脸识别治理的进路完善:从个人信息到社会公正[J]. 学术交流, 2024, (10):83-95.
[7] 林凌. 人脸识别信息保护中的"告知同意"与"数据利用"规则[J]. 当代传播, 2022, (1):108-112.
[8] 王锡锌. 个人信息国家保护义务及展开[J]. 中国法学, 2021, (1):145-166. DOI:10.14111/j.cnki.zgfx.2021.01.010.
[9] 王洪亮, 李依怡. 个人信息处理中"同意规则"的法教义学构造[J]. 江苏社会科学, 2022, (3):102-112+243. DOI:10.13858/j.cnki.cn32-1312/c.20220517.011.

[10] 王洪亮,李依怡.个人信息处理中"同意规则"的法教义学构造[J].江苏社会科学,2022,(3):102-112+243.DOI:10.13858/j.cnki.cn32-1312/c.20220517.011.