2023 9th International Symposium on Social Science (ISSS 2023)
ISBN: 978-1-60595-422-6

Research on Informed Consent Rules in the Collection of Personal Biometric Information in China

KEJIA LOU, JIAYU MAO and ZHEWEI ZHANG

ABSTRACT

Personal Information Protection Law of the People's Republic of China, which came into effect in November of 2021, formally established the legal procedures concerning informed consent in the collection of personal information. The law specifies that personal biometric information is officially considered sensitive personal information. It imposes more stringent requirements for its collection and processing in order to ensure that the information rights of the information subjects remain protected. Based on the understanding of technical risks involved in securing personal biometric information, as well as the inherent risks of information privacy in general, this paper will systematically review the current rules concerning informed consent in the collection of personal biometric information as stipulated by Chinese laws and regulations, as well as other national standards. Taking existing issues as guidance, we will also explore the compliance and regulation of the commercial use of personal biometric information under the informed consent regulations by determining the most common instances in which these rules were violated in practice.

INTRODUCTION

Personal Biometric Information is the identifiable physical and behavioral characteristics of a nature person, including specific types of facial recognition information, fingerprints, voice prints, and so on. Though its development began as early as the 1960s, it was not until the 21st century that biometric technology saw utilization on a large scale as a government tool for identifying individual citizens. In 2013, when Apple introduced Touch ID on the iPhone 5S, biometric technology was taken a step further as it transformed from a strictly government tool to a public consumer product. In recent years, the global biometric technology industry has been growing steadily. According to Transparency Market Research (TMR), a US-based market consultancy, the global biometric authentication and identification market is estimated to reach $8,798.9 million in 2026, with a compound annual growth rate (CAGR) of 16.30% during the forecast period of 2021-2026. Advancement continues with the fusion of cutting-edge technologies like machine deep learning and biometric technology, which has led to new breakthroughs in bio-metric accuracy. Meanwhile, the continuous

Kejia Lou, Jiayu Mao, Zhewei Zhang
Law School, Hangzhou City University, Hangzhou, China

improvement of the technology's cost effectiveness and security has led to the increasing diversification of biometric application scenarios. In the current global biometrics market, North America and the Asia Pacific region occupy half the market. At the same time, the market size of China's biometrics industry has also been growing rapidly in recent years, especially in the Internet finance industry and terminal retail industry.

In the Internet Age, personal biometric information is an important part of a citizen's digital identity. It is highly relevant to the information rights of an information subject, as well as personal and property safety. With the enactment of the Data Security Law (DSL) in June 2021 and the Personal Information Protection Law (PIPL) in November 2021, China's legislature has clearly recognized the need for a higher level of protection for personal biometric information. The DSL established a hierarchy of data classification and protection, while the PIPL laid out a series of special provisions concerning the collection and processing of sensitive personal in-formation, such as biometric information, to ensure its protection. Based on these laws, com-pared to general personal information, an information processor must follow more stringent rules of informed consent when collecting personal biometric information. This mainly includes the requirement for the processor to obtain the individual's separate consent before collecting such information. Furthermore, they must inform the individual of the reason behind the processing and the impact it may have on the individual's rights and interests. By instituting these mechanisms, the protection of the information subjects and their right to control their own personal biometric information is ensured.

However, within current personal biometric information collection practices, there have been repeated violations of the informed consent rule. This situation requires immediate rectification to ensure proper regulation. In light of this challenge, this paper will explore potential compliance and regulation pathways under the informed consent rule for the commercial use of personal biometric information from three levels: the internal control of enterprises, industry self-regulation, and administrative supervision. The purpose is to enhance the compliance level of personal biometric information collection by information processors under the current in-formed consent rule in the collection of such information, thus strengthening the protection of personal biometric information. This is not only a necessary precondition for eliminating the public's technological concerns regarding personal biometric information and promoting tech-nological development, but it is also necessary in the process of finding a balance between "security" and "efficiency" in the commercial use of personal biometric information.

APPLICATION RISKS OF PERSONAL BIOMETRIC INFORMATION

With the increased variety of application scenarios, personal biometric information is already present in people's lives as an "identity verification tool". For example, in the financial industry where biometric technology is most widely used, the most important use of personal biometric information is in the verification of the identity of customers. However, due to current technological limitations and the unique nature of the

procedure, the technical and inherent risks of using biometric technology as an "identity verification tool" cannot be ignored.

Biometrics are not Completely Secure

Biometric technology is still in its development stages. As such, the accompanying limitations of the technology level mean that its security cannot be completely reliable, and the technology is still at risk of being hacked. At the CCTV's 315 Evening Party on the Protection of Consumer Rights in 2017, the host showed how a 3D printed photo posted by a viewer on a social media app could be used to successfully pass a facial recognition test on a mainstream app used for facial recognition payment scenarios. In January 2019, two engineers at the Chaos Computer Club's hacker conference in Leipzig, Germany, demonstrated how a hand model created based on a photograph could be used successfully with the biometric detection technology of a vein recognition app. These types of risks associated with the use of biometric technology have led the subject of information subjects to worry about the potential security risks associated with the use of their personal biometric information once it has been collected by information processors.

Contactless Capture Takes Information Out of the Subject's Control

Some types of personal biometric information, such as facial recognition data, are often exposed directly to the outside world. This makes it easy for the personal biometric information of information subjects to be accessed without their knowledge by information processors in a contactless manner. With the continuous development of big data technology, it is not difficult to make a connection between the personal biometric information of information subjects with their other personal information. Consequentially, personal privacy will be essentially impossible in the face of big data. This is exemplified by the 2020 Facebook facial recognition class action lawsuit. [1] In this case, when a user tags other people in photos they post, Facebook will create a suggestion to tag the user's personal profile. This suggestion is derived from the facial recognition information collected by Facebook from other photos posted by the user suggested for tagging. Facebook achieves this by using facial recognition technology to turn the internet platform into a convergence channel. At the same time, however, this enables the tracking of other kinds of personal information belonging to the user based on personal biometric information. Automated technology such as this allows for the continuous processing and integration of personal biometric information. Thus, while the processor may appear to only be collecting personal biometric information, it in fact has control over all the available personal information behind that information. This may include anything from health status to financial accounts. Inevitably, this complicates the protection of personal biometric information and is undeniably a matter of great concern for society. [2]

Difficult to Effectively Remedy After a Security Incident

The high level of stability of personal physiological characteristics ensures that biometric information is naturally unique and unchangeable. This is the basis for biometric technology's ability to identify a specific individual. However, some information processors collect and process personal information as an extension of personal biometric information without the consent of the information subject. This constitutes an infringement of an individual's rights. Personal information has the dual attributes of being included under both a person's property rights and personality rights. As a kind of personality interest with property value, personal information can become legal properties. For example, information subjects may share their property rights and personal information with information processors by authorizing them to use their personal information. They could also realize the property value of personal information after it has been infringed through remedy. With the massification of internet enterprises, some large enterprises have begun to act as information processors, thereby controlling the personal biometric information of a large number of users. This is highly profitable, as they are able to transform this data into their own digital property resources through the technology of algorithms. In any event, however, the information subject does not lose the corresponding personality rights as a result of his or her act of authorizing consent to the processing of personal information by a third party. [3]

According to the PIPL's classification of biometric information as sensitive personal information, the human dignity of an individual is violated and the safety of the person and property is jeopardized should the data be leaked or used illegally. However, given the unique and unchangeable nature of personal biometric information, it is more difficult to provide effective remedies in the event of a security incident compared to other types of sensitive personal information. Once personal biometric information is leaked, one's unique and unchangeable "biometric password" is essentially made public, putting the subject of the information at risk.

INFORMED CONSENT RULES IN THE COLLECTION OF PERSONAL BIOMETRIC INFORMATION IN CHINA

Apart from the PIPL, most existing legal regulations concerning the processing of personal information in China are scattered throughout a number of laws, administrative regulations, normative documents, and standard documents. According to these laws, the processing of personal biometric information must comply with the rules concerning other more general types of personal information processing, while also complying with higher requirements specifically set for personal biometric information by some of the regulations. With regard to the collection of personal information, the current legal systems for the protection of personal information in various countries uses the informed consent rule as an effective lever to balance the protection and use of personal information, identifying it as the foundation for the legal collection of personal information. [4] In essence, the informed consent rule requires that when collecting

personal information, information processors should adequately inform individuals of what happens to their information once it is collected and obtain their explicit consent. [5]

The current rules for informed consent for the collection of personal biometric information in China are based on the PIPL, which provides the general design, and they are, supplemented by other legal norms and relevant provisions of national standards, resulting in a series of rules. Section 1 and 2 in Chapter 2 of the PIPL contains a series of rules that. deal with general personal information and sensitive personal information, respectively. In the collection of biometric personal information, information processors must not only comply with the basic consent rules for the collection of general personal information as set out in section 1 of the chapter, but they must also meet the special consent rules set out in section 2 of the chapter. In contrast to the basic consent rules for the collection of general types of personal information, the special consent rules for the collection of personal biometric information provide for the special form of informed consent, as well as an expanded scope of notification. Based on the previously established rules of informed consent which are applicable to all types of personal information collection, the rules on the informed consent for the collection of personal biometric information impose higher requirements.

Informed Rules

According to the informed consent rule, notification is the logical prerequisite for consent. Thus, the authenticity and legitimacy of consent given without adequate notification will automatically be called into question. [6] To ensure that information processor "fully inform" the subjects as required, the PIPL adopts a threefold system of "principles + general informed information + special informed information". [7] Firstly, the PIPL has adopted the principle of transparency [8] to provide the subjects with the right to be informed about the processing of their information. This is proclaimed in Article 7 of the General Regulations. In addition, Article 17 of the PIPL stipulates that before processing all types of personal information, information processors shall inform the subjects of the purpose, manner, type, and retention period of their personal information, while satisfying the dual requirements of openness and transparency in form and truthfulness, accuracy, and understandability in content. Finally, according to Article 30 of the PIPL, before collecting personal biometric information, information processors shall inform the subjects of the necessity of processing such information and its impact on their rights and interests. Compared to rules concerning informed consent of the collection of general personal information, the expansion of the scope of the notification of the collection of personal biometric information will simultaneously expand the information subjects' rights to being informed. This three-layered system, which escalates from general to specific, from abstract principles to specific rules, is the basic framework of informed consent established by the PIPL for the collection of personal biometric information.

To further ensure that personal information processors adequately inform subjects before processing personal biometric information, China has created more specific

provisions in other legal norms and national standards to bolster the informed consent during the collection of personal biometric information. For example, in Article 5.4, Subparagraph (c) of the Information Security Technology-Personal Information Security Specification (GB/T 35273-2020) (PISS), it is stipulated that the form of disclosure should be made in a separate manner before the collection of personal biometric information. [9] It adds the requirement of independence of disclosure compared to the PIPL in order to better protect the right to be informed of the subjects during the collection of personal biometric information.

Consent Rules

For the consent rules for the collection of personal biometric information, the PIPL also upgrades the formal provisions based on the consent rules for the collection of general types of personal information. In terms of consent rules in the collection of general types of personal information, Article 13, Paragraph 1, Subparagraph 1 of the PIPL specified that obtaining the consent of the subjects is one of the bases of legality for the collection and processing of personal information. This provision is in line with the understanding of the principles of personal information processing that were established in Article 1035 of the Civil Code of the P. R. China. [10] Article 14, Paragraph 4 of the PIPL also specifies that consent given by an individual means the consent is voluntary and explicit, indicating that the individual cannot be convinced, tricked or threatened to allow the processing of their personal information. Explicit consent and implied consent are two opposing concepts, meaning that the individual chooses to opt in rather than opt out. [11] Part 3, Article 4 of the Method for Determining Illegal Collection and Use of Personal Information by Apps defines "asking for user consent in a non-explicit manner such as choosing to opt into the privacy policy by default " as "without user consent". [12] Implied consent does not equal to consent. Therefore, in the rules on informing consent for all types of personal information collection, receiving explicit consent is an essential formal element of a valid admission of consent.

Following Article 14, Paragraph 4 of the PIPL, which states that "[w]here laws or administrative regulations provide that individual consent or written consent shall be obtained for the processing of personal information, the provisions thereof shall apply", Article 29 of the PIPL provides for the rule of individual consent for the collection of biometric information of individuals. According to this section, an individual’s consent must be obtained from the individual. Thus, where the law or administrative regulations require that written consent must be obtained, the provisions included therein shall apply. Facial recognition technology is the most common type of personal biometric information processing in practice. As such, the Supreme People’s Court of China issued a relevant judicial interpretation in 2021, in Article 2, Paragraph 3 of the Provisions on Several Issues Concerning the Application of Law in Hearing Civil Cases Relating to the Processing of Personal Information Using Face Recognition Technology. This article stipulates that failure to obtain the individual's separate consent or written consent to process facial information in accordance with the law is a criminal offence. This rule is also applicable to acts that infringe upon the personality rights and interests of natural

persons. Article 29 of the PIPL defines "separate consent" as "special consent" that cannot be mixed with other information, nor can the scope of the original consent be arbitrarily expanded." [13] In contrast, general consent can be considered a general “blanket consent” for future information processing. [14] The so-called "written consent", a consent given in writing, implies that the subject has the right to choose and the right to refuse the use of biometric information. [15] Therefore, when collecting personal biometric information based on user consent, special attention should be paid to whether the form of consent is complying with the requirements of "voluntary, explicit, separate, and written".

The System of Informed Consent Rules

TABLE 1. KEY ELEMENTS OF INFORMED CONSENT IN THE COLLECTION OF PERSONAL BIOMETRIC INFORMATION IN CHINA.

Type	Nature	Sources	Main content
Informed Rule	Declaratory provisions	Article 7 of the PIPL	The handling of personal information should follow the principle of openness and transparency, disclose the relevant rules for handling information, and clarify the purpose, manner, and scope of the handling of personal information.
	General Provisions	Article 17 of the PIPL	Personal information shall be handled in a conspicuous manner and disclose information in clear and understandable language truthfully, accurately, and completely of the purpose, manner, type, and period of the retention of such information, as well as the manner and procedure for exercising their rights provided by law.
		Article 18 of the PIPL	Exemptions from and delays in the duty to inform the person handling personal information (e.g. in cases where confidentiality is required by law or in emergency situations)
	Special provisions	Article 30 of the PIPL	Apart from Article 17, Paragraph 1 of the PIPL, the need for the processing of personal biometric information and its impact on their rights and interests should be disclosed.
		Article 5.4, Subparagraph c) of the PISS	The purpose, manner, and scope of the collection and retention period of biometric information shall be communicated separately to the individual prior to collection.
Consent Rule	Declaratory provisions	Article 13, Paragraph 1 of the PIPL	Obtaining consent is one of the bases of legality for processing personal biometric information.
	General Provisions	Article 14 of the PIPL	The rule of informed consent is defined in this article. Consent should be given voluntarily and explicitly by the individual on the premise of being fully informed. Laws or administrative regulations provide that

Type	Nature	Sources	Main content
			separate or written consent should be obtained for the processing of personal information, the provisions thereof shall apply.
		Article 31 of the PIPL	Where personal information such as personal information of minors under the age of fourteen is handled, the consent of their guardians shall be obtained and special rules for handling the personal information shall be established.
		Part3, Article 4 of the Method for Determining the Illegal Collection and Use of Personal Information by Apps	Where consent is obtained from an individual in a non-explicit manner prior to the collection and use of personal information, no consent has been given (i.e., explicit consent should be obtained prior to the collection and use of personal information)
	Special provisions	Article 5.4, Subparagraph c) of the PISS	Explicit consent of an individual should be obtained before the collection and use of personal biometric information.
		Article 2, Paragraph 3 of the Provisions on Several Issues Concerning the Application of Law in Hearing Civil Cases Relating to the Use of Face Recognition Technology in Handling Personal Information	When the consent obtained is not separate or written prior to the collection and use of the individual's facial biometric information, it will be deemed to be an violation of the personal rights and interests of the natural person. (i.e. the collection and use of personal facial biometric information should be conducted after by subjects' separate and written consent)
		Article 29 of the PIPL	Separate, written consent of the individual should be obtained before the collection and use of the individual's biometric information.

In summary, after elucidating the rules on disclosure and consent in the collection of personal biometric information in China, as well as explaining the connotations of their specific provisions, this article will explore the provisions of other legal norms related to the rules on disclosure and consent for the collection of personal biometric information. On the one hand, declaratory provisions are distinguished according to the abstract nature of the relevant provisions in the PIPL. On the one hand, declaratory provisions are distinguished according to the abstract nature of the relevant provisions in the PIPL. On the other hand, depending on the section in which the rules are located and the scope of application, a distinction is made between general provisions that are applicable to all types of personal information and special provisions for sensitive personal information such as biometric information. At the same time, the higher levels of requirement for informed consent for the processing of personal biometric information in other legal

norms and national standards are incorporated here into the system of rules as a supplement. To aid in this, the main contents of the current Chinese system of rules for informed consent for the collection of personal biometric information are shown in Table 1 based on two aspects: "informed" and "consent".

Exploring Compliance and Regulatory Pathways of Informed Consent Rules for Personal Biometric Information Collection

Under the Chinese system of informed consent rules for the collection of personal biometric information, incidents such as information processors not fully informing the information subjects of their information processing practices, and information processors not seeking the subjects' effective consent, make it difficult for the collection process of personal biometric information to truly protect the rights of information subjects. Thus, encouraging information processors to comply in their information collection practices, as well as ensuring effective supervision by industry self-regulatory organizations and administrative supervisory authorities under the existing rules are urgent issues that needs to be addressed in the current practice of the commercialization of biometric information.

Personal Information Processors: Strengthening the Compliance System

China's legal system on personal information protection is built around two main elements: the compliance policy and compliance management process. These establish the legal framework for the personal information protection compliance system. [16] Correspondingly, information processors' own compliance in their own processes should begin from basic compliance measures, then work towards the optimization of the substance of their internal control system. They should work to strengthen their own compliance system in response to the high-level requirements of the rules on informed consent in the collection of personal biometric information.

As a typical aspect of the compliance policy, information processors should ensure that the information they disclose to and seek consent from the information subjects during the collection and consent process complies with the formal requirements of the informed consent rule. At the same time, they should, based on their own information processing needs, design the content of the information they provide to information subjects of a personal biometric information processing agreement in accordance with the requirements of the informed rule on the premise of understanding the content of the provisions of the informed rules. After the design is completed, the information processor should conduct a self-examination in accordance with the requirements of the legal norms and promote the design of the content of the biometric agreement in the reverse direction in accordance with the evaluation results. In this way, processers can include the required content in their disclosure while avoiding omissions. [17]

The implementation of compliance policies, such as the informed consent rule, is dependent on information processors getting to the root of their own compliance management processes. Chapter 5 of the PIPL sets forth a series of obligations for

information processors. In practice, the personal information protection compliance system is an important part of the corporate compliance system. As such, information processors should conduct regular compliance audits of their personal information handling practices to assure they conduct in accordance with legal requirements. For sensitive personal information such as personal biometric information, information processors should conduct personal information protection impact assessments prior to collection to confirm the legitimacy and necessity of collecting such personal information, as well as to identify possible security risks associated with the handling of such information. In doing so, they can confirm the authenticity and completeness of the information they have communicated to the information subject. In addition, a specific compliance system should be designed for all aspects of processing of personal biometric information collected by the information processor. The information subject should also be informed, and new consent obtained in a timely manner in the event of a transfer of personal biometric information or a change in the information processor. This compliance management process guarantees the legal implementation of the compliance policy. Only by combining the two can the information processing system be fully constructed, and the desired effect of risk prevention and control be effectively achieved.

Industry Self-Regulatory Organizations & Administrative Regulators: Targeted Regulation

While information processors themselves should work to strengthen their compliance, it is clear that external forces are also needed to monitor and promote their implementation. Depending on the type of subjects, the monitoring of the collection of personal biometric information by information processors can be divided into two routes: industry self-regulation and administrative supervision.

As an auxiliary management body between information processors and administrative and regulatory authorities, industry self-regulatory organizations can create a flexible interface between internal control and external regulation by regulating business and formulating business guidelines. The specific operations can be divided into two categories: supervising information processing and formulating industry charters. Based on the group contract utilized the organization's members, industry self-regulatory organizations usually have a certain degree of self-regulatory power. [18] Compared to administrative regulatory authorities, industry self-regulatory organizations are usually more familiar with the types of personal information collected by members of their organizations and the characteristics of their handling. As such, they can remind or notify processors of any non-compliant handling of personal information in advance of administrative regulatory authorities. They can also assist processors who have been notified by administrative regulatory authorities and given a deadline for rectification. Industry self-regulatory organizations can develop industry charters to urge industry members to move towards compliance, standardization, and uniformity in the content and form of the notification of personal information handling practices given to subjects. [19] For those processors that have provided detailed information and sought clear consent in their personal biometric information collection process, certification can be

used to indicate that they have achieved a high level of compliance with the consent rules, so that other members of the organization can follow their lead and create a "product incentive". [20]

At present, the irregularities in the rules concerning informed consent in the collection of personal biometric information in practice are sufficient to illustrate the loopholes in external regulation at this stage. In this regard, with reference to Chapter 6 of the PIPL's regulations for the authorities responsible for the protection of personal information, this article suggests that the path to improve the current regulatory process should be based on the clarification of the regulatory body and the implementation of the regulatory system. Unlike the unified regulatory model represented by the EU in Article 68 of the General Data Protection Regulation where GDPR sets up the European Data Protection Board, EDPB. [21] China's personal information protection adopts a decentralized regulatory model. To obtain this, Article 60 of the PIPL continues the model of regulation put forward in article 8 of the Cybersecurity Law of the P.R. China, which established the model of "co-ordination of the Internet information department" + "decentralized supervision by relevant departments". However, at this stage, neither the cyber information department nor other industry regulators have paid attention to the special protection of personal biometric information. Even the "evaluation and disclosure" system established by Article 61, Subparagraph 3 of the PIPL in the form of a law often focuses only on the problems of personal information protection in general, such as personal information protection policies. However, it does not mention in the relevant briefings in the rules on the collection and processing of personal biometric information.

It is clear that the improvement of the regulatory regime for the processing of personal biometric information cannot be achieved overnight. Although Article 62, Subparagraph 2 of the PIPL has stipulated that special rules and standards for the protection of personal information should be formulated for new technologies such as personal biometric information, the current regulatory practice for the protection of personal information is still characterized by a "focus on the whole but not on the details". However, in the current regulatory practices used in personal information protection, this situation is still the norm, as regulators do not pay special attention to specific types of sensitive personal information. Until the relevant supporting legal norms can be further improved, administrative and regulatory authorities must rely on their own initiative to effectively regulate the collection and processing of personal biometric information. Based on the above considerations, establishing up a special governance group for the compliance work of personal biometric information processing in a regulatory body in accordance with the institutional practice of the special governance of administrative supervision in China may be suitable. For the regulatory system, the current administrative supervisory authorities should still rely on the existing legal norms based in the common means of assessment, such as "assessment and disclosure", external audit, and so on. This will allow them to provide a special governance group for personal biometric information processing. The importance of the special protection of personal biometric information should be fully appreciated

subjectively, so that the special protection of personal biometric information can be actively realized in accordance with the requirements of the present legal regulations.

CONCLUDING REMARKS

The protection of personal biometric information is not only a realistic need in China, but also a common goal for countries all over the world. Whether it is the special protection of personal biometric information stipulated by the laws of some countries or necessitating informed consent in the collection of personal biometric information in Chinese law, the aim is to achieve the special protection of the rights of information subjects to control their personal biometric information. Information processors should clearly understand that, under the rule of informed consent, the information they provide to information subjects regarding the processing of personal information is not self-aggrandizing, but rather a concrete manifestation of their social responsibility for the protection of personal information. This is, ultimately, not only the basis of trust for information subjects, but also the main goal of administrative and regulatory authorities. As the ancient Chinese philosopher Mencius famously said: "The law will not enforce itself". While countries continuously improve their legal regulations regarding the protection of personal biometric information, implementing the rules on informed consent in the collection of personal biometric information under their respective existing regulatory frameworks so as to achieve the protection of personal biometric information is inseparable from the compliance policies and regulations on compliance management by the information processors themselves. Finally, the effective exercise of industry self-regulation and administrative supervision is also necessary to achieve more comprehensive protection of information privacy rights.

ACKNOWLEDGEMENTS

This project is supported by National College Students' Innovation Training Program of China (No.202213021048).

REFERENCES

1. Biometric Authentication and Identification Market - A Global and Regional Analysis: Focus on End User, Function, Product Type, Deployment Model and Country- Analysis and Forecast, 2021-2026, retrieved from BCC RESEARCH.COM, https://www.bccresearch.com/partners/bis-market-research/global -biometric-authentication-and-identification-market.html
2. Personal Information Protection Law of the People's Republic of China (in Chinese), retrieved from NPC.GOV.CN, http://www.npc.gov.cn/npc/ c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.
3. Supreme Court declines to hear Facebook facial recognition case, retrieved from THEHILL.COM, https:// thehill.com/policy/technology/479126-supreme-court-declines-to-hear-facebook-facial-recognition-case/.

4. Han Xuzhi, Legal governance of face brushing: from identification to analysis (in Chinese), (5) J. ORIENTAL LAW, 69-79 (2021).
5. Peng Chengxin, On the dual legal nature of personal information (in Chinese), 15(06) J. Tsing- Hua University Law Journal,78-97 (2021).
6. Ji Leilei, Research on Consent Rules in Face Recognition Information Protection (in Chinese), (02) J. Police Science Research, 31-44 (2022).
7. Qi Aimin, The Authentic Thesis on Information Law (in Chinese) 76 (1st ed., Wuhan University Press, 2010).
8. Chen Feng, Wang Lirong, The function of "right to inform consent" of personal information is reviewed and improved (in Chinese), (8) J. Social Science in Guangxi, 106-111 (2021).
9. Long Weiqiu, Interpretation of Personal Information Protection Law of People's Republic of China (in Chinese) 73 (1st ed., China Legal Publishing House, 2021).
10. Personal Information Protection Research Group, International Comparative Study on the Protection of Personal Information (in Chinese) 27 (2nd ed., China Financial Publishing House, 2021).
11. Information security technology—Personal information security specification, retrieved from OPEN-STD.SAMR.GOV.CN, http://openstd.samr. gov.cn/bzgk/gb/newGbI-nfo?hcno= 4568F276E0F8346EB0FBA097AA0CE05E.
12. Huang Wei, Personality Rights of the Civil Code Made Up of the P.R. China (in Chinese) 199 (1st ed., Law Press·China, 2020).
13. Long Weiqiu, Interpretation of Personal Information Protection Law of People's Republic of China (in Chinese) 64 (1st ed., China Legal Publishing House, 2021).
14. Notice on the issuance of the "Method for Determining the Illegal Collection and Use of Personal Information by APP", retrieved from CAC.GOV.CN, http://www.cac.gov.cn/2019-12 27/c15789864556866 25.htm.
15. Shi Jiayou, Liu Siqi, Personal Information Protection in Face Recognition Technology: The Construction of Dynamic Consent Mode (in Chinese), (2) J. Law and Economy, 60-78 (2021).
16. Han Xuzhi, The Dilemma and Solution of Informed- consent Rule in Personal Information Protection—On the Relevant Provisions of the Personal Information Protection Law (in Chinese), (1) J. Business and Economic Law Review, 47-59 (2021).
17. Fu Weiming, The legal protection model of personal biometric information and China's choice (in Chinese), 22(6) J. Ecupl Journal, 78-88 (2019).
18. Mao Yixiao, Research on Data Protection Compliance System (in Chinese) 2022(2) J. Journal of National Prosecutors College, 84-100 (2022).
19. Xiao Xue, Cao Yufei, Research on Compliance Evaluation for the Personal Information Protection Policies of Social Applications (in Chinese) 44(03) J. Information Studies: Theory & Application, 91-100(2021).
20. Gu Gongyun, Economic Law Course (in Chinese) 59 (3rd ed., Shanghai People's Publishing House, 2013).
21. Z Zhang Yanfeng, Qiu Yi, Research on Compliance of Privacy Policy of Mobile Reading APP in China Under Hard Rules (in Chinese) 42(01) J. Journal of Modern Information, 167-176(2022).
22. Li Yanshun, Discussion on the Problems of Infor- mation Privacy Protection in Big Data Age (in Chinese) 25(04) J. Henan Social Sciences, 67-73(2017).
23. General Data Protection Regulation of the European Union, retrieved from GDPR-INFO.EU, http://gdpr-info.eu.