Proceedings of the 5th International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/2026.37286

The Scope and Processing of Sensitive Information: Based on the Legislation Personal Information Protection

Heming Yin

Law School, East China University of Political Science and Law, Shanghai, China
hmingyin@outlook.com

Abstract. With the development of the digital economy, more and more data will be created and used, so protecting sensitive personal information is now a serious problem. But the scope of sensitive personal information listed in Article 28 of China's Personal Information Protection Law issued in 2021 still remains ambiguous in practice and thus problems have arisen in enforcement and compliance. This study will analyze the current legal framework and address this ambiguity and the formalism of mandatory consent through comparative study of EU's General Data Protection Regulation and America's California Privacy Rights Act, as well as a case study. This study argues that China should adopt purposive interpretation to judge sensitivity based on risks of damage regardless of the category of data, refine the current opt-in consent structure to guarantee users' genuine voluntariness and strengthen corporate accountability by setting a personal information protection impact assessment, thus bridging the gap between legislation itself and real-world data processing situations.

Keywords: sensitive information, comparative law, PIPL, GDPR, CPRA

1. Introduction

In the digital economy, people start to lay more emphasis on sensitive personal information because this kind of information is highly related to people's privacy and asset security. The Personal Information and Protection Law (hereinafter referred to as "PIPL") was enacted in 2021 and the definition of sensitive personal information has been made to distinguish itself from other personal information. However, the definition in Article 28 still cannot fully adapt to every case, like the case of Luo v. a technology company [1]. The court protected the users' rights based on the fact that the information the English-learning app obtains was not necessary when the app provided services and the app failed to provide other log-in methods if the users refused to provide their own portrait like the occupation, study aims and the level of English. But the court did not answer whether the "portrait", the combination of insensitive personal information was sensitive or not.

This essay will deal with the problem of the vagueness of the sensitive personal information and the limitation of the mandatary consent. This essay will use the advantages of the legislation in the U.S. and the EU for references., as interpreted by the Court of Justice of the European Union in C-184/20, the scope of the definition of sensitive personal data has been broadened by Article 9 of General Data Protection Regulation (hereinafter referred to as "GDPR"). The court considered that

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.37286

the processing of personal data, from which sensitive personal data could indirectly be deduced by cross-referencing that personal data with other data, comes within the prohibition of Article 9(1) [2]. Meanwhile, according to U.S.'s California Privacy Rights Act (hereinafter referred to as "CPRA"), the disclosure of personal information that is mandated by the contract to those disclosures that are made to service providers is limited. Users' consent must be obtained if the relevant information will be shared with entities other than service providers [3]. By integrating these insights, this essay argues that China can adopt purposive interpretation to interpret and confirm whether something is sensitive personal information or not and give more limitation to the content of authorization.

The contribution of this essay lies in fulfilling Chinese protection framework of sensitive information and propose specific ways through analyzing the development of Chinese legislation and the comparison between China, EU and America.

2. The development of Chinese legislation of sensitive information

The development of China's legal system of sensitive information protection has been proceeding gradually and has moved from fragmented regulations to a more unified system. While the enforcement of PIPL has taken measures to close loophole in the Cybersecurity Law and Electronic Commerce Law, there are still some questions remained to be discussed and interpreted.

2.1. Cybersecurity Law (2017), Electronic Commerce Law (2019) and Criminal Law

The Cybersecurity Law enforced on June.1st, 2017 and the Electronic Commerce Law enforced on Jan.1st, 2019 both fails to clarify the differences between the sensitive information and insensitive information.

The former one, the Cybersecurity Law only defines what is personal information in the Article 76, paragraph 5. "Personal information" refers to any information whether stored electronically or by other means, either independently or combined with some other information to successfully identify a specific individual, including the person's name, date of birth, identity certificate number, etc.

Before the PIPL defined the term, the vague definition of "sensitive information" first appeared in one interpretation issued by the Supreme People's Court in 2017. According to Interpretation Article 5 and Criminal Law Article 253, if the circumstances are serious, the processors can be sentenced to imprisonment for no more than three years and if the circumstances are especially serious, the processors can be sentenced to imprisonment for no less than three years but not more than seven years. The serious circumstances include providing or selling more than 50 pieces of "highly sensitive" information (seriously limited to only 4 kinds of information) or more than 500 pieces of "sensitive" information or more than 5,000 personal information. The tiered structure illustrates that whether the infringement is serious or not depends on the sensitivity of the personal information

2.2. Personal Information Protection Law (2021)

The definition of sensitive personal information was not established until the PIPL was enacted in 2021. Article 28 both involves summary and enumeration ways of interpreting what is sensitive information.

According to Article 28, sensitive personal information means if such information leaks or is illegally used, it can easily infringe upon an individual's right to privacy and cause harm to their

DOI: 10.54254/2753-7048/2026.37286

personal or property safety. To make it more concrete, it includes information such as biometric identification, personal whereabouts, personal information of minors under 14 and etc.

Beyond that, PIPL also establishes the rules and restrictions when processing this kind of information. Before information processors process this kind of information, specific purposes and sufficient necessity must be reached and strict protection measures must be taken. The following step is to conduct the personal information protection impact assessment and make all the records. During the assessment, the purposes, the methods of processing, the impacts on individuals' rights and interests and security risks shall be confirmed and checked carefully. Most importantly, the whole reports should be kept for at least three years. After that, the information processors must get respectively mandatory consent from the individuals and tell these individuals the necessity of processing and how it will affect their personal rights and interests. The court will even hold them criminally accountable where their conduct meets the threshold of a crime under the Criminal Law.

2.3. The drawbacks of Personal Information Protection Law

Didi, the Chinese version of Uber, a carhailing platform, was fined as much as 8.026 billion yuan in July, 2022, which has been the highest fine since the PIPL was enacted. Didi was penalized for illegally processing millions of users' personal information, including huge amounts of sensitive personal information like precise location tracking information, the ID card numbers and so on.

When it comes to the drawbacks of today's legislation, there are mainly 2 aspects.

The first one is the vagueness of the definition of sensitive personal information [4]. Though it involves summary and enumeration ways of interpreting, it still has uncertainty.

From the perspective of interpretation, by literal interpretation,the seven types of information listed clearly in Article 28 must be sensitive personal information. However, by purposive interpretation, whether a certain kind of information is judged as sensitive personal information should be based on the standard of risk of damage. It means that if a kind of information has low risk of damage, it shouldn't be considered as sensitive personal information despite the fact that it belongs to this category. And if it doesn't belong to this category, it should be considered as sensitive personal information as long as it has high risk of damage [5]. This two ways of interpretation conflicts.

From the perspective of characteristic, in Article 28, the words "could easily lead to" are strongly subjective due to the lack of objective standards, which makes it difficult to weigh the risk of damage [6]. Also, the sensitivity of personal information isn't fixed and invariable, which means it heavily depends on the processing background [7]. For example, some insensitive personal information, such as the browsing history and purchase history, may be converted to sensitive personal information through comprehensive analysis. It hasn't made clear how to deal with this kind of circumstance in law.

The second one is the limitation of the rules of processing sensitive personal information. Though what is sensitive personal information has been defined, its core rules (mandatory consent) still fail to realize its function effectively in practice. In the background of more and more complicated data processing, there is information asymmetry between the processor and the individuals. In one way, the individuals sometimes fail to realize the value of their personal information, which means what they consider insensitive or unimportant one can be converted to sensitive one through multiple processing where new goals or results are derived from old ones [8]. In another way, when the individuals face complicated and professional privacy policy, it's hard for them to make fully informed and voluntary consent, leading to formalism. Though the judgement of the case of Luo v. a technology company protects the users' privacy, China isn't a common-law country, so when the

DOI: 10.54254/2753-7048/2026.37286

court deals with similar cases, they can only take the former case as references. It's still necessary for China to make legislation in this problem.

3. Comparison of current legislation between China, the United States and EU

As shown by the analysis of China's legislative drawbacks above, it reveals that viewing similar problems form more grand international perspectives should be done first. The approaches taken in the United States and the EU should be analyzed and compared for the scope of sensitive personal information, legal bases for processing and enforcement and remedies, providing references for improving China's current legal framework.

3.1. Current legislation in the United States

3.1.1. Scope of sensitive personal information

The way CCPA treats insensitive personal information and sensitive personal information is the same. When it comes to CPRA, sensitive personal information includes the following types of data and is regulated in the same way as under CCPA: genetic data, biometric information, health information and another three types of information. What's different from CCPA is that the scope of such information in CPRA also contains specific types of that such as precise geolocation, the content of communications and other information which meets the requirement of the FCC's order. However, CPRA doesn't list web browsing history and application usage history as sensitive as FCC's order, where attention should be paid to [3].

3.1.2. Legal bases for processing

The CCPA can collect and use personal information without users' consent, while under CPRA, sensitive personal information should only be used after obtaining the user's consent for other purposes besides "necessary to provide the services that a common consumer can reasonably expect" or for other specified business purposes [9]. Therefore, the businesses can mandate in the terms that insensitive personal information can be collected and used. But in terms of disclosure of personal information, CPRA has placed stricter limitations on the disclosure of personal information, and only service providers can be disclosed; at the same time, service providers are prohibited to share information with entities other than service providers [3].

Additionally, the CPRA considers opt-in consent as an affirmative authorization and offers the consumers the right to opt-out [10]. The CPRA also makes special regulation to protect the minors under 16: the sale of personal information of consumers under 16 requires opt-in consent and the consumers more than 13 years old are given the right to opt out of such sales [11].

3.1.3. Enforcement and remedies

On July.1st, 2023, the California Privacy Protection Agency (CPPA) and the California Attorney General began enforcement of CPRA, and thus provided the time and opportunities for the businesses to revise or update their respective privacy policies to meet the requirements of the latest revision of CPRA [12]. CPRA offers consumers the right to opt-out whenever they want [10].

DOI: 10.54254/2753-7048/2026.37286

3.2. Current legislation in EU

3.2.1. Scope of sensitive personal information

Modifications have been made to the special-purpose types of personal information by the GDPR. According to Article 9(1), a closed list of special types of data has been established and the scope of protection for these has been expanded to cover three more types related to gene, biometrics and sex in summary. Apart from that, there are another 5 kinds of sensitive personal information respectively related to racial, political, beliefs, trade union membership and health in summary. GDPR uses more concreate enumeration to address the debates on which category of data should be considered as sensitive personal information by regulation, instead of by directive. Member states can't set new types of sensitive personal information under Directive 95/46/EC any longer [7]. As interpreted by the Court in C-184/20, the GDPR has expanded the scope of the definition of such data in Article 9 of Regulation (EU)2016/679. The court considered that the processing procedure, from which sensitive personal data could indirectly be deduced by cross-referencing that personal data with other data, comes within the prohibition of Article 9(1).

3.2.2. Legal bases for processing

Under the GDPR, Article 6 establishes the legal bases for the processing of sensitive personal information. In Article 6, contract necessity and legitimate interests are the most important factors when the court judge whether the lawfulness of processing is reached.

Based on the settled case-law of the Court of Justice, objective necessity is required during the processing for the execution of the contract, which means that the related terms written as "useful" for its execution of the contract has no referential value during the valuation. It should be confirmed that no feasible or less intrusive options exist, given the reasonable expectations of the data subject [13].

At the same time, Article 6(1)(f) also set a three-step test (three cumulative conditions) to ensure the processing is lawful and the legitimate interests won't be violated. Firstly, the controller or any third parties who receive the data pursues a legitimate interest. Secondly, the processing is necessary for obtaining the legitimate interests. Thirdly, the individuals' basic rights and freedoms do not outweigh that interests.

Both standards are focused on the objective necessity, but the latter also needs to weigh the balance between the interests of different parties.

When it comes to the consent structure, GDPR requires that consent should be informed, which means that data subjects must be fully aware of the processing, like the processing purposes, what data is collected, the way of using data, whether it will cause harm to the subjects and so on [3]. And the controllers are required to notify the data subjects that they can withdraw the prior consent any time they want. The withdrawal should complies with the processing carried out under the prior consent before withdrawal. As the GDPR is an opt-in system for the legal basis of consent, it does not require the controllers to highlight their right to opt-in. These above notices will ensure a genuine, freely given consent.

3.2.3. Enforcement and remedies

GDPR establishes a Data Protection Impact Assessment (DPIA) and regulates that new high-risk data-processing activities likely to impact the rights and freedoms of individuals substantially should

DOI: 10.54254/2753-7048/2026.37286

undergo such an assessment [14]. GDPR doesn't enumerate all the situations in which a DPIA is compulsory, but among the enumeration, there does list one occasion: large-scale handling the special types of data. Due to the characteristic of the current era, the capacity of data is booming and more and more processing of sensitive data meets the criterion of the necessity of conducting a DIPA [7].

Under GDPR, a Data Protection Officer (DPO) should be designated by the data controller if the main processing targets consist of huge amounts of special types of data [15]. The DPO is obliged to make sure that the processing complies with the GDPR and other forms of law. Its duty also includes giving advice on how to implement it and check whether such implementation has been operated.

3.3. Comparative analysis

In terms of web browsing history and application usage history, CPRA doesn't list it as sensitive personal information against FCC's order. Comparatively, according to C-184/20, the processing, from which sensitive personal data could indirectly be deduced by cross-referencing that personal data with other data, comes within the prohibition of Article 9(1). In this way, web browsing history and application usage history can be considered as sensitive one with the combination of other personal information [2]. Generally, this kind of history is sensitive personal information that PIPL regulates because it may violate the personal dignity in practice.

In terms of the juveniles, CPRA only establishes a more strict structure when the processors sell under 16's personal information (opt-in model for the minors under 16), but it doesn't list it as sensitive personal information. GDPR puts emphasis on protecting children's data in the Recital 38, but it doesn't list it as sensitive personal information either. However, PIPL particularly lists the minors under 14's information as sensitive one based on age, which is totally different from other countries' legislation. It means that age is the only factor that needs to be taken into account during judgement and there is no need to valuate normal standards on this occasion.

In terms of the rules of the consent for processing such information, the GDPR mandates an opt-in structure where controllers must obtain explicit consent before processing sensitive data, with consent defined as voluntary, explicit, well-informed and unambiguous. Comparably, the CPRA requires opt-in consent for sensitive information, but the scope of data can be applied to is narrower than under GDPR. It also gives the consumers the right to opt-out whenever they want. The PIPL follows an opt-in structure similar to GDPR, which requires separate consent for sensitive information and mandates that consent should be "voluntary and explicit" [16]. However, PIPL's related consent rules face practical challenges that the existing information asymmetry between processors and individuals causes users' consent to be reduced to formalism. The GDPR's opt-in structure is reinforced by DPO and DPIAs for large-scale sensitive data processing, while CPRA's opt-out structure depends more heavily on consumers' own initiative. This comparison reveals that while GDPR and PIPL share similar opt-in architecture, while PIPL's implementation is limited due to the absence of robust enforcement mechanisms comparable to GDPR's DPO and DPIA.

4. The development direction of protection towards sensitive information

Given that the PIPL just came into effect in 2021, it's not practical to conduct large-scale revisions to the PIPL in such short period. At present, some improvements to the structure will be made by judicial interpretation and guiding cases.

Firstly, specify the range and kind of sensitive personal information that will be collected. Article 28 should be interpretated through purposive interpretation, which means that if a kind of

DOI: 10.54254/2753-7048/2026.37286

information has low risk of damage, it shouldn't be considered as sensitive personal information despite the fact that it belongs to this category. Though the data listed explicitly in Article 28 do belong to sensitive personal information in most cases, extra room should be made for the exceptions that haven't occurred up till now. Whether the leakage or illegal use of the personal information poses a threat to the dignity or personal and property security of the individuals should be the most authoritative standard and the listed categories should just serve as references [4].

Referring to the cases of C-184/20 in the CJEU, the rule is that when processing personal data, if sensitive information can be indirectly deduced by cross-referencing, it falls under the scope of Article 9(1) of the GDPR. For example, algorithms can be employed to process the web-browsing history and application-use records of users to form users' profiles thoroughly, which consititute sensitive personal information. In such conditions, the standard should be whether the processing procedures or results causes a high level of risk of infringing the users' interests, regardless of what category of the raw data falls in.

Secondly, the consent mechanism must be refined to ensure the consent itself is genuinely voluntary and informed. The exception of the conditions when the processor can process personal information under Article 13(1) and (2) should be interpreted strictly. Like the Guiding Case No. 265 of the Supreme People's Court, it should only apply when the processing is objectively necessary for providing a service's main function, meaning the service cannot be performed without it. This exception should not justify collecting sensitive information for unnecessary purposes like forming users' profile for future advertising and products promoting, where the court considered that collecting user portrait information was not necessary for the provision of the educational app's basic services. Furthermore, businesses should not offer condition service based on the user's consent for processing unnecessary information and should provide other login methods, since it is a kind of indirect compulsion.

For sensitive information, the requirement for "separate consent" must be enforced strictly. It should not be buried within long privacy policies. Instead, businesses should be required to emphasize the related terms of the permission of sensitive personal information in the long privacy policies or send separate requirement to ask for consent for following processing activities, ensuring the user's agreement is specific and informed.

Thirdly, corporate accountability and authority's supervision should be strengthened. China can adopt the Personal Information Protection Impact Assessment (PIA) with clear guidelines to ensure risks associated with processing sensitive data are correctly identified and addressed [16]. The duties of the DPO and the requirement for a PIA, as introduced in the GDPR, provide a good reference for enhancing compliance in large-scale sensitive data processing [7].

Finally, enforcement can't be neglected either. Regulatory authorities should issue guiding cases more frequently to help the judges broaden their judicial reasoning. Courts should apply the fault presumption rule (Article 69 of the PIPL) more effectively. In private information infringement cases, courts may use factual presumptions to reduce the plaintiff's burden of proof, particularly when confirming the link between the processing and the damage consequence, thus providing more accessible judicial remedy [17]. This way can help to overcome the problems the individuals face when trying to prove a processor's fault or the connection between data processing and damage consequence.

5. Conclusion

This essay has examined the legal framework of how to define, regulate and protect the sensitive personal information under China's current PIPL under the background of a more and more

DOI: 10.54254/2753-7048/2026.37286

advanced and prosperous digital economy. Generally speaking, the two problems mentioned are a lack of clarity in the definition in Article 28 and the absence of a mandatory consent mechanism in practice. Based on the analysis of other countries' legislation, comparisons with the EU's GDPR and America's CPRA and consideration of judicial practice such as the Luo v. Technology Company case, this study argues that China should adopt a purposive interpretation of sensitivity, refine the consent process to ensure that genuine and voluntary consent is obtained and formalism is avoided to a large extent and strengthen corporate accountability by impact assessments and the following enforcement. By studying the strength, China can identify shortcomings and bridge the gap between current legislation and the data processing in practice in this era.

References

[1] Supreme People's Court News Office. (2025). Guiding case No. 265: Luo v. a technology Co., Ltd. (dispute over privacy rights and personal information protection). *Supreme People's Court Website*. Retrieved from https://www.court.gov.cn/shenpan/xiangqing/474481.html.
[2] Stock, M. (2023). The CJEU expands the scope of the definition of sensitive personal data in the GDPR: Case C184/20 Vyriausioji Tarnybines Etikos Komisija. *Business Law International, 24*(1), 93-97.
[3] Jordan, S. (2022). Strengths and weaknesses of notice and consent requirements under the GDPR, the CCPA/CPRA, and the FCC broadband privacy order. *Cardozo Arts & Entertainment Law Journal, 40*(1), 113-174.
[4] Ding, X. (2025). Interpretive reconstruction of the sensitive personal information protection system. *China Legal Science, 2*, 168-187.
[5] Wang, L. (2022). Basic issues in the protection of sensitive personal information: In the context of interpretation of the Civil Code and the Personal Information Protection Law. *Contemporary Law Review, 1*, 3-14.
[6] Zhao, X. (2023). *Defining the scope of sensitive personal information*. Master thesis of Southwest University of Political Science and Law.
[7] Quinn, P. (2021). The difficulty of defining sensitive data—the concept of sensitive data in the EU data protection framework. *German Law Journal, 22*(8), 1583–1612.
[8] Guo, C. (2024). Reflection and revision of the rules for processing sensitive personal information. *Tribune of Political Science and Law, 42*(3), 102–113.
[9] Supra note 4, §1798.121(a) of CPRA.
[10] Supra note 4, §1798.140(h) of CPRA.
[11] Supra note 4, §1798.120(c) of CPRA.
[12] Latzer, A. (2022). Complying with new and existing biometric data privacy laws. *Journal of Business, Entrepreneurship and the Law, 16*, 201–232.
[13] Meta Platforms Inc., Formerly Facebook Inc., Meta Platforms Ireland Limited, Formerly Facebook Ireland Ltd., Facebook Deutschland GmbH v Bundeskartellamt. (2023). Intervener: Verbraucherzentrale Bundesverband e.V. *Reports of Cases before the Court of Justice and the Court of First Instance, 1*, 1-25.
[14] Supra note 1, at art. 35(a) of GDPR.
[15] Supra note 1, at art. 37 of GDPR.
[16] Cheng, X. (2021). On the rules for processing personal information in China's Personal Information Protection Law. *Tsinghua Law Journal, 15*(3), 55-73.
[17] Li, Z. (2023). Application of the rules for protecting private information: An interpretive theory centered on Article 1034(3) of the Civil Code. Master thesis of East China University of Political Science and Law.