ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

China

Status of Consent for Processing Personal Data

MAY 2022

AUTHORED BY

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

Hunter Dorwart

Policy Counsel for Global Privacy, Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTOR

Kemeng Cai

Partner, Han Kuhn Law

ACKNOWLEDGEMENTS

This Report benefitted from contributions and editing support from Elizabeth Santhosh.

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION

This report summarizes the roles played by consent and related provisions, including alternatives to consent, in China's data protection framework and highlights provisions which can serve as indicators for convergence of laws and regulations in this area across Asia Pacific.

Consent requirements have always been central to China's framework for protecting personal information ("**PI**") and were already predominant in the patchwork of different laws and regulations that provided for data protection before China's omnibus data protection law, the Personal Information Protection Law ("**PIPL**"),[1] came into effect on November 1, 2021.

The predominance of consent requirements in China's data protection framework may have been a response to public backlash against technology companies that sold and processed PI in an unregulated manner. In particular, a number of scandals—including one that resulted in the death of a high school student whose data was sold and misused by a company—generated outrage among the Chinese public and led to widespread complaints that consumer protection laws were inadequate to prevent harms resulting from the processing of PI.[2]

Since 2020, the legal infrastructure for protection of PI in China has been based on Article 1035 of the Civil Code, which enshrines a right to the protection of personal data which is explicitly linked to an individual's consent. The PIPL builds on this right by establishing consent as one of several legal bases for the collection and processing of PI in a structure which resembles that of the GDPR.

Thus, China's legal system has profoundly evolved over the past two years and is converging towards international standards, particularly in relation to consent (e.g., that consent must be free, can be withdrawn, and must take certain forms in special circumstances, and that notice must be given) and exceptions or alternatives to consent.

However, at the same time, differences remain, including, notably, the absence of a concept of "legitimate interests" like that of the GDPR[3] or other major data protection laws internationally, such as Singapore's Personal Data Protection Act following amendments in 2020. The decision not to incorporate this concept into the PIPL suggests that regulators may still be uneasy about permitting Big Tech companies to determine, in the first instance, whether a given purpose for processing PI is reasonable.

It is not possible at this stage to affirm that China's legal system is undergoing a transformation towards a principally accountability-based framework like some of its neighbors. However, it is important to recognize that the PIPL only recently took effect and that the scope of this law and its articulation with other laws which "complicate data governance"[4] will be clarified in the coming years through implementing regulations, advisory or enforcement decisions. Even within this constrained perimeter, there may still be opportunities for convergence.

2. CHINA'S DATA PROTECTION FRAMEWORK

The main provisions of Chinese law for processing of personal data are found in the Civil Code, the PIPL, the Personal Information Security Specification ("**Security Specification**"), the Cybersecurity Law ("**CSL**"), and other administrative regulations.

---

[1] Hunter Dorwart, Gabriela Zanfir-Fortuna, and Clarisse Girot, "China's New Comprehensive Data Protection Law: Context, Stated Objectives, Key Provisions" *Future of Privacy Forum blog* (August 20, 2021), available at https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/

[2] Xu Yuan, "Complaints about data abuses by businesses are increasingly driven by consumers in China" *mlex* (March 26, 2021), available at https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/data-privacy-and-security/complaints-about-data-abuses-by-businesses-are-increasingly-driven-by-consumers-in-china

[3] See GDPR, Article 6(1)(f).

[4] Mingli Shi, "China's Draft Privacy Law Both Builds On and Complicates Its Data Governance" *New America blog* (December 14, 2020), available at https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-privacy-law-both-builds-on-and-complicates-its-data-governance/

2.1. Civil Code

China's Civil Code – which was officially adopted on May 28, 2020 and came into force on January 1, 2021 – introduced an independent book on Personality Rights,[5] including a chapter entitled "Rights to Privacy and Protection of Personal Information."[6] This chapter, among others, defines the scope of privacy and PI protection, the rules for PI protection, the obligations of PI handlers, and the rights of individuals.

The default rule under the Civil Code is that organizations and individuals are prohibited from processing PI, unless the right holder over such PI expressly consents to the processing, or the processing is otherwise provided by law.[7] This provision introduces into Chinese law a requirement that there must be an explicit basis in law for collecting and processing of PI. Article 1035 of the Civil Code further enshrines consent as the primary legal basis for collection, use, and disclosure of PI, unless otherwise provided by laws or administrative regulations.[8]

2.2. Personal Information Protection Law ("PIPL")

The PIPL – which was passed in August 2021 and took effect in November 2021 – builds on relevant provisions of the Civil Code. Specifically, Article 13 of the PIPL a requirement, which is similar to and likely modeled on equivalent provisions in the GDPR, introduces several legal bases for processing of PI[9] by "PI handlers."[10] Although consent remains an important legal basis under this provision,[11] the provision also lists six other bases as alternatives to obtaining individuals' consent, namely:

- handling PI where necessary to:
  - conclude or perform a contract to which the individual is an interested party or where necessary to comply with relevant labor regulations or the execution of a collective contract to implement necessary human resources supervision (e.g., employee data);[12]
  - fulfill statutory duties and responsibilities or statutory obligations;[13] or
  - respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;[14]
- handling PI within a reasonable scope to implement news reporting, supervision of public opinion, and other such activities for the public interest;[15]
- handling, within a reasonable scope, PI that has been publicly disclosed by an individual or other legally disclosed information, unless the individual expressly refuses or if there is a major influence on individual rights and interests;[16] or
- other circumstances provided in laws and administrative regulations.[17]

---

[5] Civil Code, Book IV.
[6] Civil Code, Chapter VI
[7] Civil Code, Article 1033(5).
[8] Civil Code, Article 1035.
[9] Note that pursuant to Article 4 of the PIPL, "**personal information**" refers to information (howsoever recorded) which relates to identified or identifiable natural persons but does include anonymized data, and "handling" includes collecting, storing, using, processing, transmitting, providing, disclosing, and deleting PI.
[10] Note that Article 73(1) of the PIPL defines "**personal information handlers**" as organizations or individuals that autonomously decide the purposes or methods for handling of PI.
[11] PIPL, Article 13(1).
[12] PIPL, Article 13(2).
[13] PIPL, Article 13(3).
[14] PIPL, Article 13(4).
[15] PIPL, Article 13(5).
[16] PIPL, Article 13(6).
[17] PIPL, Article 13(7).

2.3. PI Security Specification ("Security Specification")

The Personal Information Security Specification, GB/T 35273-2020 ("**Security Specification**") – which was issued in March 2020 and implemented in October 2020 – is not legally binding. However, as Chinese authorities use the Security Specification as a standard to assess organizations' compliance with other legal guidelines and regulations, the Security Specification functions as a *de facto* requirement for businesses.

The Security Specification lays out granular guidelines for obtaining consent and for collecting, using, and disclosing PI. In contrast to other legal instruments such as the Civil Code and PIPL, the Security Specification specifies many more alternative legal bases to consent for processing of PI and provides exceptions to consent not seen in other regulatory documents in China.

2.4. Cybersecurity Law ("CSL")

The CSL – which was passed in November 2016 and took effect in June 2017 – requires providers of network products or services which collect user information to inform their users of such collection and obtain users' consent thereto.[18]

If the user information collected includes PI, then the network product or service provider is also subject to more stringent requirements,[19] including:

- obtaining the consent of the persons whose data is collected;
- publishing rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information; and
- abiding by the principles of legality, propriety, and necessity.[20]

The CSL also prohibits network operators from providing PI to third parties without the consent of the data subject, unless the data has been irreversibly de-identified.[21]

These provisions were not affected by the adoption of the Civil Code, the PIPL, and the Security Specification, but there remains uncertainty as to how the CSL interacts with these subsequent legal instruments.

2.5. Sectoral regulations and guidelines

Prior to the enactment of the Civil Code, which expressly provides that PI may be processed pursuant to legal bases other than consent, companies in China had to rely on strict consent for all processing of PI. Detailed regulatory guidelines therefore exist for consent but not for legal bases for processing PI. Most of these guidelines predate adoption of the PIPL, and some also predate the Security Specification and the CSL.

a. Financial services

The Implementation Measures of the People's Bank of China for Protecting Financial Consumers' Rights and Interests ("**PBOC Specification**") – the most important regulation in protection of personal financial information – requires banks and payment institutions to obtain explicit consent from data subjects for processing their personal financial information[22] and explicitly specify the purposes, means

---

[18] CSL, Article 22(3).

[19] CSL, Article 22(3). Note that Article 76(5) of the CSL defines "**personal information**" as any information that alone or in combination with other information is sufficient to identify a natural person.

[20] CSL, Article 41. Note that Article 76(1) of the CSL defines a "**network**" as a system comprising computers or other information terminals and related equipment that follows certain rules and procedures for gathering, storing, transmitting, exchanging, and processing information. Article 76(3) defines "**network operators**" as network owners, managers, and network service providers.

[21] CSL, Article 42.

[22] Order No. 5 [2020] of the People's Bank of China (Implementation Measures of the People's Bank of China for Financial Consumer Protection) ("**PBOC Specification**"), Article 29.

and scope for collecting and using such information.[23] Where banks and payment institutions obtain such consent through standard terms, these terms must explicitly state the purposes and means of collecting consumer financial information as well as the content and scope of use in language as plain as possible.[24]

The Administrative Measures for Credit Investigation Services also require credit reporting agencies to obtain consent of the data subject and clearly inform that person of the purpose of collecting credit information unless the information is disclosed in accordance with other laws and regulations.[25]

b. Mobile applications

There are also numerous guidelines that specify the circumstances and measures under which consent is valid for collection of PI by mobile applications.

For instance, the draft Information Security Technology Guidelines for Personal Information Notice and Consent[26] – released by the National Information Security Standardization Committee (TC260) – make recommendations for consent mechanisms for certain scenarios including, among others, the Internet of Things (IoT), Software Development Kits (SDKs), personalized advertising, processing of minors' PI, online financing services, connected vehicles, and online shopping. Generally, consent cannot be obtained through coercive, deceptive, or illegal methods, and there are rules around when controllers can bundle consent for multiple processing items.

In April 2021, the Ministry of Industry and Information Technology ("**MIIT**") and the State Administration of Market Regulation ("**SAMR**") issued draft Interim Provisions on the Administration of Personal Information Protection of Mobile Internet Application, under the guidance of the Cyberspace Administration of China ("**CAC**").[27] These guidelines reinforce the rule that apps cannot collect users' PI without consent and impose stringent requirements, among others, against the common practice of "bundled consent" by applying a strict necessity test. When providing users' PI to the third party, apps must provide users with certain information on the third, including identity and contact details and the purpose and method of processing. Separate notification is also required for processing of sensitive PI.

Additionally, on January 5, 2022, the CAC released a draft Regulation on the Management of Mobile Internet Application Information Services[28] which further solidifies regulatory guidance towards app developers but imposes additional rules on mobile app stores.

c. Automotive sector

Chinese regulators have also issued guidance for the automotive sector, particularly in the area of smart vehicles and connected cars.[29] For instance, multiple ministries released "Several Provisions on Vehicle Data Security Management (Trial)"[30] in August 2021, and the MIIT issued its "Guidelines for the Construction of the Internet of Vehicles Network Security and Data Security Standard System" in February 2022.[31] Both documents provide detailed guidance as to the circumstances in which operators of connected cars would be permitted to rely on consent as a legal basis for processing PI.

---

[23] PBOC Specification, Article 31.

[24] PBOC Specification, Article 31.

[25] Order No. 4 [2021] of the People's Bank of China (Measures for the Administration of Credit Reporting Services), Articles 12-13.

[26] Available at http://std.samr.gov.cn/gb/search/gbDetailed?id=AC81A866CD7D59BFE05397BE0A0A95E2

[27] "Notice on Issuing the "Regulations on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications"" *Netcom China on WeChat* (March 22, 2021), available at https://mp.weixin.qq.com/s/euwT3utf231iRxxGdUH82w

[28] Available at http://www.cac.gov.cn/2022-01/05/c_1642983962594050.htm

[29] Chelsey Colbert, "Update: China's Car Privacy and Security Regulation is Effective on October 1, 2021" *Future of Privacy Forum* blog (August 27, 2021), available at https://fpf.org/blog/update-chinas-car-privacy-and-security-regulation-is-effective-on-october-1-2021/

[30] Available at http://cac.gov.cn/2021-08/20/c_1631049984897667.htm

[31] Available at https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2022/art_e36a55c43a3346c9a4b31e534b92be44.html

3. CONSENT AND PRIVACY SELF-MANAGEMENT IN CHINA'S DATA PROTECTION LAW

Consent plays a central role in Chinese data protection law and is the longest established legal basis for processing PI under Chinese law.

However, with the enactment of the PIPL in 2021, Chinese law now provides several alternative legal bases for processing PI, which are placed on an equal level to consent. The addition of these alternatives reflects a debate within China on the role of consent within the country's data protection architecture and recognizes the need to provide businesses with greater flexibility as to how and when they can process personal data (especially employee and other business data), while protecting individuals from harm.

There is no clearly stated position as to why consent has been made a foundation of China's data protection architecture. While the Civil Code couches consent within the framework of individual personality rights, no explanation has been provided as to why consent is prioritized over other legal bases. There is also no stated position from a regulator, government, or other organization as to whether there is a need to rethink the role of notice and consent in China. However, practitioners and legal scholars widely perceive that consent is both insufficient (e.g., data subjects' consent may not be meaningful where there is an imbalance of power) and too rigid (e.g., consent should not be required for the pursuit of legitimate interests like anti-fraud).

Consent has also played a large role in the enforcement patterns of Chinese regulators thus far.[32] Practitioners in China spend a considerable amount of time advising organizations on their consent collection and management processes, including notifications through privacy policies and other statements. Both the CAC and the MIIT have issued numerous warnings to entities indicating that their consent policies are in violation of Chinese law.

4. CONDITIONS FOR CONSENT

4.1. Definition and forms of consent

Consent is not defined in the CSL, the PIPL, or the Civil Code. By contrast, the Security Specification defines consent as an act whereby a natural person who is identified by or associated with PI (the "**PI Subject**") expressly authorizes the specific processing of his/her PI.[33]

a. Security Specification

The Security Specification distinguishes between "**consent**" and "**explicit consent**."

"**Consent**" appears to encompass both express and implied or deemed consent, as the note to this definition explains that authorization could be given through a positive act (e.g., explicitly giving consent) or a passive act (e.g., remaining in an area after having been informed that PI is being collected there).[34]

"**Explicit consent**" is defined as an act whereby a PI Subject explicitly authorizes the specific processing of his/her PI by making a written statement, including by electronic means, or an oral statement, or by making an affirmative action of his/her own accord.[35] Examples of affirmative action include checking or clicking "agree," "send," or "dial;" filling in a form; or where a PI Subject provides PI of his/her own accord.[36]

It also appears that in both cases, consent must be informed, as the Security Specification requires the organization or person that is in a position to determine the purpose and means of processing PI ("**PI**

---

[32] See "SANCTIONS AND ENFORCEMENT."
[33] Security Specification, paragraph 3.7 read with paragraph 3.3.
[34] Security Specification, paragraph 3.7, note 1.
[35] Security Specification, paragraph 3.6.
[36] Security Specification, paragraph 3.6, note 1.

Controller") to explicitly inform PI Subjects of the purpose, method, scope, and other rules for PI processing, when seeking the PI Subjects' consent.[37]

In practice, operators usually obtain explicit consent from users by displaying links to their privacy policies upon initial registration or start page of mobile applications or web services and requiring users to affirmatively click on buttons or checkbox stating "confirm" or "registration." These requirements are lower than those under the GDPR.

For collection of sensitive PI, the explicit consent must be a specific and clear expression of intention voluntarily made by the PI Subjects on the basis of complete knowledge.[38]

b. PIPL

The PIPL distinguishes between "**individual consent**,"[39] "**written consent**," and "**separate consent**." These terms are not defined.

Where PI is handled based on individual consent, the individual must give consent under the precondition of full knowledge, and in a voluntary and explicit statement.[40]

The PIPL does not specify what constitutes written consent. References to written consent in PIPL appear to anticipate that other laws and regulations may require consent in writing for certain uses of PI,[41] notably for certain handling of sensitive PI.[42]

The PIPL requires separate consent where:

- it is required by other laws or administrative regulations;[43]
- PI handers provide PI to third parties;[44]
- PI handers disclose or use PI collected by video devices or personal identification devices in public places for purposes other than safeguarding public safety;[45]
- PI handers process sensitive PI;[46]
- operators provide PI to a party outside of China.[47]

The PIPL does not specify what constitutes separate consent. However, the draft Online Data Security Management Regulations – which were released for public comment in November 2021 but are not yet in effect – provide a definition of separate consent which requires the data handler, when carrying out specific data handling activities, to obtain consent for each item of PI individually. [48]

Note that the draft Online Data Security Management Regulations also provide that separate consent for data transfers may be obtained upon initial collection if the organization notifies the individual of the transfer at the time of consent and thereafter, carries out the transfer under the terms specified to the individual.[49]

---

[37] Security Specification, paragraphs 4(c) and 5.4(a).

[38] Security Specification, paragraph 5.4(b). Sensitive PI is discussed in further detail under "CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA."

[39] See PIPL, Articles 13-15.

[40] PIPL, Article 14.

[41] See PIPL, Articles 14 and 29.

[42] PIPL, Article 29.

[43] PIPL, Article 1.

[44] PIPL, Articles 23 and 25.

[45] PIPL, Article 26.

[46] PIPL, Article 29.

[47] PIPL, Article 39.

[48] Draft Online Data Security Management Regulations, Article 73(8).

[49] Draft Online Data Security Management Regulations, Article 36.

c. Sectoral regulations

Under existing regulations and enforcement decisions on mobile applications, operators are required to obtain users' consent to operators' privacy policies through proactive actions (e.g., checking a box, clicking "I agree," etc.). Operators are prohibited from using pre-checked boxes to obtain consent to their privacy policies, and operators that do so will be deemed to have collected PI without users' consent. Note that the regulators' position on using pre-ticked boxes in other contexts is less clear and may need to be analyzed on a case-by-case basis.

4.2. Withdrawal of consent

The PIPL provides that where PI is handled on the basis of individual consent, individuals have a right to rescind their consent, and PI handlers must provide a convenient way for individuals to withdraw their consent.[50] Withdrawal of consent does not affect the validity of the PI processing activities that were carried out based on the individual's consent prior to the withdrawal.[51]

A PI handler is also prohibited from refusing to provide products or services on the basis that an individual has rescinded consent, except where handling PI is necessary for the provision of products or services.[52]

4.3. Prohibition on bundled consent

Prohibitions on "bundled consent" are found in the Security Specification, which stresses the importance of voluntary consent and prohibits PI processors from requiring data subjects to give consent for processing of their PI as a precondition for receiving products and services, and the State Administration for Market Regulation's Measures for the Supervision and Administration of Online Transactions,[53] which came into force in May 2021. Market regulators are increasing their oversight of internet businesses (which have been avid users of "bundle consent") to minimize the number of "clicks" required before individuals could use their online services.

a. Security Specification

Under the Security Specification, where a product or service provides a number of "business functions" that require collection of PI, a PI Controller may not "force" a PI Subject to accept business functions or requests for collection of PI.[54] In particular, a PI Controller may not bundle business functions so that the PI Subject is required to give bulk consent that covers collection of PI for business functions that the PI Subject does not use and has not requested.[55] Affirmative action on the part of the PI Subject to activate a business function is required before a PI Controller may initiate collection of PI.[56]

PI Controllers must also create convenient methods for PI Subjects to opt out of business function.[57] Once a PI Subject has chosen not to authorize, or has deactivated or exited a business function, the PI Controller may not frequently request for consent[58] and may not suspend any other business function for which the PI Subject has opted in voluntarily nor reduce the service quality of any other business function.[59]

---

[50] PIPL, Article 15.

[51] PIPL, Article 15.

[52] PIPL, Article 16.

[53] Available at https://gkml.samr.gov.cn/nsjg/fgs/202103/t20210315_326936.html

[54] Security Specification, paragraph 5.3. Note that paragraph 3.17 of the Security Specification defines a "**business function**" as a service type that meets the specific needs of PI Subjects. Examples include maps and navigation services, online car hailing, instant messaging, online communities, online payments, news and information, online shopping, express delivery, and transport ticketing (Security Specification, paragraph 3.17, note 1).

[55] Security Specification, paragraph 5.3(a).

[56] Security Specification, paragraph 5.3(b).

[57] Security Specification, paragraph 5.3(c).

[58] Security Specification, paragraph 5.3(d).

[59] Security Specification, paragraph 5.3(e).

Lastly, PI Controllers are also prohibited from demanding that PI Subjects authorize the collection of PI solely for the purposes of raising service quality, improving user experience, developing new products or enhancing security.[60]

b. "Core" versus "ancillary" business functions

More broadly, at the policy level, China's laws and regulations differentiate between consent required for "basic business functions" versus "ancillary business functions" of a product or service. This distinction draws heavily from the GDPR experience on necessity for contract.

"Core functions" usually refer to the functions essential for the products or services provided by the network operator that satisfy the principal needs of data subjects for using the products or services.

"Ancillary functions" are usually additional functions to these products and services, or functions aimed at improving user experience. For example, an ordinary payment function may be deemed to be a core function of a payment application, while a payment function using facial recognition may be deemed to be an ancillary function. Similarly, an online shopping function may be deemed to be a core function of an e-commerce platform, while location-based shopping or social interaction with people nearby may be deemed to be ancillary functions.

The purposes for distinguishing between "core" and "ancillary" functions are to implement the principles of necessity and data minimization and to restrict forced or bundled collection of personal data in excessive amounts. Operators may therefore deny the provision of services to data subjects who refuse to provide the PI necessary for the core functions of such services. In contrast, operators may not force users to launch ancillary functions or bundle ancillary functions and core functions together to enlarge the scope of PI collection. The controller may further not incentivize the data subject to consent by guaranteeing better quality service or increased security in return for authorized consent for a specific business function. Moreover, if the subject ceases to use a specific business function, the controller cannot continue to use the PI previously collected. This provision has been taken over in the PIPL.

4.4. Whether access to services may be conditional on consent

Under the PIPL, a PI handler may not refuse to provide products or services on the basis that an individual does not give consent to handling of his/her PI, except where the processing of PI is essential for providing the products or services.[61] This reflects the distinction between core and ancillary functions found in the Security Specification (see above).

5. TRANSPARENCY AND NOTICE

CSL and Civil Code require operators to:

- disclose their rules relating to collection and use of PI; and
- state the purpose, means, and scope of such collection and use.[62]

The PIPL further requires operators to:

- explicitly inform the individual of the following matters in clear and plain language:
  - the identity and contact information of the PI processor;
  - the purpose and means of processing PI, and the type and retention period of the processed PI;
  - the means and procedures by which the individuals are to exercise the rights provided herein.

[60] Security Specification, paragraph 5.3(f).
[61] PIPL, Article 16.
[62] CSL, Article 41; Civil Code, Article 1035.

  - other matters shall be notified in accordance with the provisions of laws or administrative regulations; and
  - any changes to the above matters;[63] and
- keep their policy or rules easily available and storable/downloadable for data subjects.

Regarding privacy policies, the Security Specification clarifies that if a product or service only provides one business function that collects and uses PI, a PI Controller may inform the PI Subjects by way of a "PI protection policy." If a product or service provides several business functions that collect and use PI, the PI Controller should, in addition to providing the PI protection policy, inform the PI Subjects of the purpose, method and scope of the collection and use of such PI when starting to collect particular PI so that the PI Subjects can thoroughly consider the specific impact before giving consent.[64]

6. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

Chinese law recognizes special categories of data and imposes heightened processing obligations on organizations that process such data.

The PIPL defines sensitive information as PI that, once leaked or illegally used, may easily cause harm to the dignity of natural persons or grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking, etc., as well as the PI of minors under the age of 14. [65]

Notably, unlike the GDPR and similar laws, which provide a closed list of "special categories" of personal data,[66] the PIPL has an open list of sensitive data based on the notion of harm and the potential for discrimination against individuals, taking into account a wide range of factors.

The PIPL further differs from the GDPR in that the scope of sensitive information under the PIPL expressly includes financial information and location data but does not expressly include PI related to criminal convictions and offenses.

Under the PIPL, PI handlers may only process sensitive PI for specific purposes and when sufficiently necessary.[67] Except where the PIPL provides otherwise,[68] PI handlers must also obtain separate consent[69] and notify individuals of the necessity for handling sensitive PI, and effect of such handling on the individuals' rights and interests. These provisions raise challenges for compliance due to the lack of a clear definition of "separate consent" and the level of detail required under the PIPL's notification obligations.

The Security Specification requires a PI Controller to obtain explicit consent from the PI Subject before collecting sensitive PI[70] and provides the following list of examples of categories of data that would qualify as sensitive data to those in the PIPL: [71]

- identification card numbers;
- personal biometric information;
- bank account numbers;
- communication records and content;

---

[63] PIPL, Article 18.

[64] Security Specification, paragraph 5.4(a), note 1. For further information on requirements for privacy policies, see paragraph 5.5 of the Security Specification.

[65] PIPL, Article 28.

[66] See GDPR, Article 9.

[67] PIPL, Article 28.

[68] PIPL, Article 30.

[69] PIPL, Article 29.

[70] Security Specification, paragraph 5.4(b).

[71] Security Specification, paragraph 3.2.

- property information;
- credit information;
- tracking records;
- lodging information;
- physiological health information;
- transaction information; and
- PI of children under 14 years old.[72]

6.1. Children

The Security Specification[73] and the PIPL[74] treat the PI of children under 14 years old as sensitive PI. Both also require parental consent for processing of the PI of minors under the age of 14. Controllers have an affirmative duty to ensure that they obtain consent in these circumstances, regardless of whether they have reason to believe that the individual is under 14 years old.

Note that the age of majority in China is 18,[75] though a minor aged 16 or above whose main source of support is the income from his own labor is deemed to have full capacity for performing civil juristic acts.[76]

a. Security Specification

Before collecting the PI of minors of or above the age of 14, PI Controllers must obtain explicit consent from the minors or their guardians; for minors under the age of 14, explicit consent from their guardians is required.[77]

b. PIPL

The PIPL expressly states that the PI of minors under the age of 14 qualifies as sensitive PI.[78] PI handlers who handle the PI of minors under the age of 14 must not only obtain the consent from the minor's parent or guardian but also formulate specialized PI handling rules.[79]

c. Sectoral regulations

Under the Regulations on the Protection of Children's Personal Information Online, controllers must meet additional requirements when processing PI of minors.[80] The regulations notably provide additional clarification on some key provisions in the PIPL and the Security Specification.

6.2. Cookie, Internet of Things, Online Tracking

Neither the Security Specification nor the PIPL expressly state that cookies or information obtained through IoT or online tracking qualify as sensitive PI (however, note that the Security Specification identifies *web browsing history* as an example of sensitive PI[81]). Whether such information would qualify as sensitive depends on whether disclosure of information would lead to harm to the data subject.

---

[72] Security Specification, paragraph 3.2, note 1. Note that Annex B to the Security Specification provides further information on identifying methods and types of sensitive PI.
[73] Security Specification, Articles 3.2 and 5.4(d).
[74] PIPL, Article 28.
[75] Civil Code, Article 17.
[76] Civil Code, Article 18.
[77] Security Specification, paragraph 5.4(d).
[78] PIPL, Article 28.
[79] PIPL, Article 31.
[80] Protection of Children's Personal Information Online.
[81] Security Specification, Annex B.

6.3. Biometric data

a. Security Specification

The Security Specification imposes additional notice requirements for "**personal biometric information**," which includes genes, fingerprints, voice prints, palm prints, auricles, iris, and facial features. [82] Before collecting personal biometric information, PI Controllers must inform the PI Subjects separately of the purpose, method, scope, storage time and other rules for collecting and using such information and must obtain explicit consent from the PI Subjects.[83]

b. PIPL

The PIPL also treats biometric data as sensitive PI.[84] Sensitivity around biometric information has also informed policymaking with respect to facial recognition. Note that under the PIPL, organizations can use facial recognition technologies in public places only when it is necessary to preserve public safety, unless the individual consents.[85]

Other institutions in China have chimed in on the legal ramifications of facial image collection. The Supreme People's Court issued a Judicial Interpretation Against Misuse of Facial Recognition Technology to address the issue. [86]

6.4. Genetic data

The Security Specification identifies genetic data as an example of personal biometric information[87] which would be classified as sensitive PI.[88]

The Regulations of the People's Republic of China on the Administration of Human Genetic Resources also require prior informed consent in writing for collection, preservation, and cross-border transfer of genetic data.[89]

6.5. Financial information

a. Security Specification

The Security Specification identifies bank account, property, transaction, and credit information as examples of sensitive PI.[90]

b. PIPL

The PIPL also treats financial information as sensitive PI.[91]

c. Sectoral regulations

The PBOC Specification provides for different categories of "personal financial information" ("**PFI**"), i.e., PI processed in the provision of financial services or products. Under the PBOC Specification, PFI is

---

[82] Security Specification, paragraph 5.4, note 3.
[83] Security Specification, paragraph 5.4(c).
[84] PIPL, Article 28.
[85] PIPL, Article 26.
[86] Laney Zhang, "China: Supreme People's Court Issues Judicial Interpretation Against Misuse of Facial Recognition Technology" *Library of Congress Global Legal Monitor* (August 19, 2021), available at https://www.loc.gov/item/global-legal-monitor/2021-08-15/china-supreme-peoples-court-issues-judicial-interpretation-against-misuse-of-facial-recognition-technology/
[87] Security Specification, paragraph 5.4, note 3; Annex B.
[88] Security Specification, paragraph 3.2, note 1.
[89] Regulations of the People's Republic of China on Administration of Human Genetic Resources, Articles 9 and 12.
[90] Security Specification, paragraph 3.2, note 1; Annex B.
[91] PIPL, Article 28.

divided into three categories (C3, C2, C1) depending on the level of sensitivity.[92] This approach of distinguishing between different levels of sensitivity of information is seen in other sectors, including in sectors that process non-PI.

6.6. Location data

a. Security Specification

The Security Specification identifies records of whereabouts[93] and precise location information[94] as examples of sensitive PI.

b. PIPL

The PIPL treats individual location data as sensitive PI. [95]

7. CONSENT FOR CROSS-BORDER DATA TRANSFERS

Under Chinese data protection law, cross-border transfers of PI have been interwoven with the obligation to obtain consent.

Under the PIPL and related measures, PI handlers must provide a detailed list of information to data subjects regarding the transfer of their data overseas and obtain "separate consent" for the transfer.

There is ambiguity as to the circumstances in which this requirement may apply, which may make compliance impracticable. Although recent draft administrative measures[96] have specified further interpretation of separate consent for cross-border transfers, China's framework for data transfers still appears to be consent-centric.

7.1. Cross-border transfer rules and security assessments

For a PI handler to transfer PI outside of the People's Republic of China, PI handler must:

- notify the individual of the foreign recipient's name, method of contacting the foreign recipient, the purpose and method of handling PI, the category of PI involved, and procedures for the individual to exercise his/her rights under the PIPL with the foreign recipient;[97]
- obtain the individual's separate consent;[98] and
- meet any of the following conditions:
  - passing a safety assessment by the CAC;
  - obtaining certification on PI protection from by a qualified certification institution recognized by the CAC;
  - entering into an agreement according to the template formulated by the CAC with the overseas recipient to specify the rights and obligations of both parties, and supervising the compliance of recipient's PI processing activities;
  - satisfying other conditions provided by laws, administrative regulations, or provisions of the CAC.[99]

---

92 See PBOC Specification, Article 33.
93 Security Specification, paragraph 3.2, note 1.
94 Security Specification, Annex B.
95 PIPL, Article 28.
96 Draft Online Data Security Management Regulations, Article 36.
97 PIPL, Article 39.
98 PIPL, Article 39.
99 PIPL, Article 39.

When conducting a security assessment for the transfer, the CAC will take into account the legal environment of the recipient and whether the recipient can ensure an adequate level of protection through appropriate safeguards.

Under Chinese law, a security assessment may be required under specific circumstances.

Firstly, if the controller qualifies as a critical information infrastructure operator or a special controller recognized under a sectoral regulation ("**CIIO**"), then the controller may only transfer data related to the critical information infrastructure or as specified in the sectoral regulation for business necessity and must undergo a security assessment before the transfer. Additionally, under the PIPL, controllers that process a "large" quantity of PI must also undergo such an assessment for transfers of their PI.[100] Further guidance has defined this as an organization that processes PI of more than 1 million individuals.[101]

Secondly, controllers that process important data or cumulatively transfer the PI of 100,000 individuals or sensitive PI of 10,000 individuals must also undergo a security assessment to transfer such information out of China. The Draft Online Data Security Management Regulations define important data as any data that is leaked or misused would harm the national security or public order of China or the legitimate rights and interests of individuals.[102]

8. SANCTIONS AND ENFORCEMENT

Chinese authorities are generally active in enforcing consent requirements and have launched numerous campaigns against non-compliant privacy policies, entities that have failed to obtain valid consent, and entities that excessively collect information or bundle consent.

For instance, the MIIT has recently announced a broad investigation campaign to specifically target entities that fail to obtain consent properly or otherwise illegally collect PI.[103] This investigation has produced concrete results, with over 100 entities fined or suspended for their data collection activities.

Under normal circumstances, the MIIT or the CAC will notify an individual company that they are in noncompliance with the law and give the organization a chance to rectify before issuing any penalties. In some circumstances, these regulators will release a public list to announce the closure of an investigation and put companies on notice that they are in noncompliance. In serious circumstances, regulators will take more remedial measures such as inspections.

8.1. Civil Code

Violations of the personality rights in the Civil Code may lead to penalties defined under Chinese administrative law. The Civil Code itself does not provide for remedies or penalties *per se*, but under Chinese law, courts may adjudicate and determine the level of damages for these violations. Litigation under these cases continues to increase in China.[104]

8.2. CSL

Failure to comply with the CSL's consent requirements may give rise to sanctions, including warnings, confiscation of unlawful gains, fines, suspension of operations, and cancellation of business licenses.[105]

---

[100] PIPL, Article 40.

[101] Draft Data Export Evaluation Measures, Article 4(3).

[102] Draft Online Data Security Management Regulations, Article 73(3).

[103] "App notification on violations of user rights and interests" *China Information Security on WeChat* (February 18, 2022), available at https://mp.weixin.qq.com/s/UT86qv7vMeGpLWu-QW-qLQ

[104] Hunter Dorwart, "Platform regulation from the bottom up: Judicial redress in the United States and China" *Policy & Internet*, 1– 22 (2022), available at https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.289

[105] CSL, Article 64.

8.3. PIPL

Where PI is handled in noncompliance with the PIPL, the relevant authorities are empowered to do the following:

- order correction;
- confiscate unlawful income;
- order provisional suspension or termination of provision of service for application programs that have unlawfully handled PI;
- impose fines of not more than 1 million yuan where correction is refused; and
- impose fines of between 10,000 and 100,000 yuan on the person directly responsible person and other directly responsible personnel.[106]

Additionally, where the unlawful acts are committed in grave circumstances, the relevant authorities are empowered to do the following:

- impose a fine of not more than 50 million yuan, or 5% of annual revenue;
- order the suspension of related business activities or cessation of business for rectification;
- report to the relevant competent department for cancellation of corresponding administrative licenses or cancellation of business licenses;
- impose fines of between 100,000 and 1 million yuan on the person directly responsible and other directly responsible personnel;
- prohibit responsible persons from holding positions of director, supervisor, high-level manager, or PI protection officer for a certain period. [107]

PI handlers may also be required to pay compensation where handling infringes PI rights and interests and results in harm.[108]

9. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT

There is currently no general provision in the PIPL or other legal instruments permitting a PI handler to collect and process PI without consent if the PI handler undertakes a risk impact assessment, such as the "legitimate interests" basis for processing under the GDPR. It is nonetheless possible that further administrative regulations will provide an equivalent basis for collection and processing of PI in future.

That said, the inclusion of a legal basis for processing of employee data without consent under Article 13(2) of the PIPL is notable in that it recognizes at least one circumstance where it may be impracticable or inappropriate to obtain consent but where processing of PI should nevertheless be permitted for ordinary business functions. This provision built on precedents found in local regulations like the recent Shenzhen data regulation,[109] which expand exceptions to consent for employers to process employees' data for certain purposes.

9.1. Impact assessments under the PIPL

Notwithstanding the lack of a comprehensive "legitimate interests-type" ground in the PIPL, the PIPL requires PI handlers to undertake a risk-based PI impact assessment in situations where PI handling may have "a major influence on individuals."[110]

---

[106] PIPL, Article 66.

[107] PIPL, Article 66.

[108] PIPL, Article 69.

[109] Sherry Gong, Tommy Liu, Mark Parsons, "Shenzhen finalizes the local data regulation" *JD* Supra (August 6, 2021), available at https://www.jdsupra.com/legalnews/shenzhen-finalizes-the-local-data-5831971/

[110] PIPL, Article 55(5).

This assessment must include the following:

- whether or not the PI handling purpose, handling method, etc., are lawful, legitimate, and necessary;[111]
- the influence on individuals' rights and interests, and the security risks;[112]
- whether protective measures undertaken are legal, effective, and suitable to the degree of risk. [113]

Such assessments are used by controllers to evaluate the risk of certain processing activities as well by regulators to assess those activities when doing so is necessary under the law. For instance, controllers must compile such risk assessments for transfers of PI outside of China, taking into account the ability of the recipient to ensure an equivalent level of protection as recognized under Chinese law, including whether the transfer agreement specifies adequate protection obligations in its terms and conditions, and whether the recipient or entrusted processor has put in place technical and organizational measures to ensure security.

Controllers have an obligation to ensure, either through contractual terms or through physical inspections, that their recipients will process the PI within the scope, purpose and means stipulated by the contract and, if the processing is based on consent, accepted by the notified data subject.

Additionally, it is unclear to what extent controllers must engage in risk balancing when processing data pursuant to an exception to consent, such as for health emergencies.

10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

10.1. PIPL

The PIPL provides that PI may be handled without the need to obtain individual consent in the following circumstances:

- where handling is necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts;[114]
- where handling is necessary to fulfill statutory duties, responsibilities, or obligations;[115]
- where handling is necessary to respond to sudden public health incidents or protect natural persons' lives and health or security of their property in an emergency; [116]
- where PI is handled, to the extent reasonable, for news reporting and media supervision or similar activities in the public interest; [117] and
- where data subjects have already disclosed the PI themselves or where the PI has otherwise already been lawfully disclosed, within a reasonable scope in accordance with the PIPL; [118] and
- in other circumstances provided by laws and administrative regulations. [119]

---

[111] PIPL, Article 56(1).
[112] PIPL, Article 56(2).
[113] PIPL, Article 56(3).
[114] PIPL, Article 13(2).
[115] PIPL, Article 13(3).
[116] PIPL, Article 13(4).
[117] PIPL, Article 13(5).
[118] PIPL, Article 13(6). Note that this basis is unavailable where the individual clearly refuses (PIPL, Article 27). PI handlers are also required to obtain consent where handling of PI that has already been disclosed would have a major influence on individual rights and interests (PIPL, Article 27).
[119] PIPL, Article 13(7).

As the PIPL only took effect in late 2021, there is currently little guidance as to the interpretation of these legal bases.

10.2. Security Specification

The Security Specification provides that a PI Controller does not need to obtain consent from PI Subjects for collection or use of their PI which is:

- in connection with the fulfillment by the PI Controller of obligations under laws and regulations;[120]
- directly related to:
  - national security or national defense; [121]
  - public security, public health or major public interests; [122]
  - criminal investigations, prosecutions, trials or execution of court decisions; [123]
- for the purpose of safeguarding the life, property, or other significant legitimate rights and interests of the PI Subjects or other individuals, and it is hard to obtain consent from the PI Subjects; [124]
- in respect of PI which the PI Subject has disclosed to the public; [125]
- essential to the signing and performing of a contract requested by the PI Subject; [126]
- collected from legally and publicly disclosed information, such as legal news reports and government information disclosure; [127]
- essential to maintaining safe and stable operation of the product or service provided, such as the discovery and handling of product or service failures; [128]

or where the PI controller is:

- a news agency, and the collecting and using of PI are essential for it to carry out legitimate news reporting;[129] or
- an academic research institution, and the collecting and using of PI are essential for it to carry out statistics or academic research for public interests, provided that the PI contained in the results is de-identified when it makes the academic research or the descriptive results available. [130]

10.3. Other regulations

The draft Online Data Security Management Regulations extend certain of the PIPL's lawful bases for handling PI in the specific context of data transfers. Data controllers that transfer data pursuant to a mechanism under Article 38 of the PIPL do not need to choose one if the transfer is necessary to perform or conclude a contract, or to protect the health, life, or property of the data subject.[131]

Note that transfers of PI for law enforcement purposes may be subjected to heightened restrictions under Chinese law. The PIPL and the Data Security Law explicitly state that controllers may not transfer PI of individuals within China to foreign law enforcement or judicial bodies without the approval of

---

[120] Security Specification, paragraph 5.6(a).
[121] Security Specification, paragraph 5.6(b).
[122] Security Specification, paragraph 5.6(c).
[123] Security Specification, paragraph 5.6(d).
[124] Security Specification, paragraph 5.6(e).
[125] Security Specification, paragraph 5.6(f).
[126] Security Specification, paragraph 5.6(g). Note that a privacy policy would not be deemed to be a contract for this purpose.
[127] Security Specification, paragraph 5.6(h).
[128] Security Specification, paragraph 5.6(i).
[129] Security Specification, paragraph 5.6(j).
[130] Security Specification, paragraph 5.6(k).
[131] Draft Online Data Security Management Regulations, Article 35.

Chinese authorities. This requirement stands even if the foreign body is requesting such information pursuant to a law enforcement investigation.

ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879 ABLI.ASIA | INFO@ABLI.ASIA

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

1350 EYE STREET NW | SUITE 350 | WASHINGTON DC 20005 FPF.ORG | INFO@FPF.ORG