Asia Pacific Law Review

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rplr20

Whose data is it anyway? An empirical analysis of online contracting for personal information in China

Qin Zhou

To cite this article: Qin Zhou (2023) Whose data is it anyway? An empirical analysis of online contracting for personal information in China, Asia Pacific Law Review, 31:1, 73-99, DOI: 10.1080/10192557.2022.2117484

To link to this article: https://doi.org/10.1080/10192557.2022.2117484

ASIA PACIFIC LAW REVIEW
2023, VOL. 31, NO. 1, 73–99
https://doi.org/10.1080/10192557.2022.2117484

Routledge
Taylor & Francis Group

Whose data is it anyway? An empirical analysis of online contracting for personal information in China

Qin Zhou

Faculty of Law, Macau University of Science and Technology, Macau, People's Republic of China

ABSTRACT

China's data governance has garnered global attention. An important part of data governance is the protection of personal data. Many believe that the newly issued Personal Information Protection Law (PIPL) can improve the protection of personal information in China. However, the merits of this specialized law rest in part on empirical exams. This paper explores whether the PIPL can solve the issues existing in online contracting for personal information in China. It firstly introduces provisions related to contracting for personal information before the promulgation of the PIPL. It then identifies three critical issues regarding online contracting for personal information in China after reviewing 202 online peer-to-peer lending platforms' terms of service and privacy policies. These issues include privacy policies that are not readily accessible, the substantial variation between terms of service and privacy policies pertaining to personal information collection, processing, sharing, and protection, and the bias of contractual terms. The paper further discusses whether the PIPL can help address three issues considered in the survey results. It argues that, even though the new law looks promising and may help address some of the issues in online contracting for personal information, its effectiveness ultimately depends on its enforcement and consumers' reaction to changes in the way firms contract for personal information. Therefore, this paper also calls for more empirical studies on China's personal information protection.

KEYWORDS

Personal information; privacy policies; terms of service; content analysis; China

I. INTRODUCTION

China's digital industry has grown to become one of the world's most vibrant industries. In 2020, the country's digital economy grew rapidly amid the COVID-19 pandemic, accounting for nearly 40 per cent of the GDP.[1] One of the factors contributing to China's growing digital economy is its large netizen population. Almost one billion Chinese have been online by 2020, including 86 per cent of those using digital payments.[2]

CONTACT Qin Zhou zhouqin@must.edu.mo

[1]Yujie Xue, 'China's Digital Economy Surges in 2020 Aimed Pandemic, Making Up Nearly 40 Per Cent of Country's GDP' *South China Morning Post* (27 April 2021) <https://www.scmp.com/tech/policy/article/3131286/chinas-digital-economy-surges-2020-amid-pandemic-making-nearly-40-cent> accessed 29 August 2021.

[2]China Internet Network Information Center (CINIC), *The 47th China Statistical Report on Internet Development (*第47次《中国互联网络发展状况统计报告》*)* (Report, February 2021) 17 <http://www.cac.gov.cn/2021-02/03/c_1613923423079314.htm> accessed 1 April 2021.

However, the country has a reputation for weak protection of personal data and privacy.[3] Some Chinese internet companies have an insouciant disregard for the rights of data subjects and personal data security.[4] As a result, public concern about the protection of personal data has been growing, especially in facial recognition surveillance, the controversial social credit system, and the development of other privacy-invading technologies.[5]

In recent years, China has made significant progress in data-related legislation. The Cybersecurity Law, enacted in 2016, is the first law that defines personal information, affirms users' rights to rectification, and requires network operators to protect users' personal information and notify users when data breaches occur.[6] Furthermore, the Cybersecurity Law extends the requirements of protecting personal information to all businesses operating computerized information networks.[7] Despite the Cybersecurity Law's mention of personal information protection provisions, those provisions are not addressed systematically.[8] The promulgation of the Civil Code,[9] the Data Security Law,[10] and the Personal Information Protection Law ('PIPL')[11] demonstrate the continued emphasis in China on the protection of personal information. The three laws establish a more comprehensive legal framework for data governance in China. They empower individuals with the right to access, correct and delete their personal information; impose various obligations on data handlers for personal information collection, processing and protection; and provide legal remedies in personal information infringement cases.

Many studies have been on China's legislative developments of personal data protection.[12] Recently, some have paid particular attention to the impact of China's data-related legislation on cybersecurity, cross-border data flows, and digital assets

[3]See Juro Osawa and Eva Dou, 'China's Top Web Browsers Leave User Data Vulnerable, Group Says' *The Wall Street Journal* (28 March 2016) <https://www.wsj.com/articles/chinas-top-web-browsers-leave-user-data-vulnerable-group-says-1459198802> accessed 12 January 2021.

[4]For example, Robin Li, the chief executive officer of Baidu, declared that 'if [Chinese people] are able to trade privacy for convenience, for safety, for efficiency, in a lot of cases they are willing to do that'. See Xinmei Shen, 'Chinese Internet Users Criticize Baidu CEO for Saying People in China are Willing to Give Up Data Privacy for Convenience' *South China Morning Post* (28 March 2018) <https://www.scmp.com/abacus/tech/article/3028402/chinese-internet-users-criticize-baidu-ceo-saying-people-china-are> accessed 21 January 21.

[5]Tiffany Li, 'China's Influence on Digital Privacy Could Be Global' *The Washington Post* (7 August 2018) <https://www.washingtonpost.com/news/theworldpost/wp/2018/08/07/china-privacy/> accessed 13 January 2021.

[6]Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法) (promulgated by the Standing Committee of the National People's Congress (SCNPC) on 7 November 2016, effective on 1 June 2017), Arts 41–43, 49 and 76(5) (hereinafter 'Cybersecurity Law').

[7]Ibid, Art. 2.

[8]Ibid, Art. 11. The primary purpose of Cybersecurity Law is to ensure cybersecurity, safeguard cyberspace sovereignty, national security, and public interests, and protect citizens and entities' legitimate rights. Personal information protection is part of network information security, stipulated in Chapter four of the Cybersecurity Law.

[9]Civil Code of the People's Republic of China (中华人民共和国民法典) (promulgated by the National People's Congress (NPC) on 28 May 2020, effective on 1 January 2021), book 4, ch 6 (hereinafter 'Civil Code').

[10]Data Security Law of the People's Republic of China (中华人民共和国数据安全法)(promulgated by the SCNPC on 10 June 2021, effective on 1 September 2021).

[11]Personal Information Protection Law of the People's Republic of China (中华人民共和国个人信息保护法) (promulgated by the SCNPC on 20 August 2021, effective on 1 November 2021).

[12]See, e.g. Zhizheng Wang, 'Systematic Government Access to Private-Sector Data in China' (2012) 2 *International Data Privacy Law* 22; Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspective* (OUP, 2014) ch 7; Hanhua Zhou, 'Exploring An Incentive-Compatible Personal Information Protection Regime (探索激励相容的个人数据治理之道)' (2018) 2 *Chinese Journal of Law (*法学研究*)* 3; Fuping Gao, 'Protection of Personal Information: From Individual Control to Social Control (个人信息保护: 从个人控制到社会控制)' (2018) 3 *Chinese Journal of Law (*法学研究*)* 84; Feng Yang, 'The Future of China's Personal Data Protection Law: Challenges and Prospects' (2019) 27 *Asia Pacific Law Review* 62; Philip Andreas Weber, Nan Zhang and Haiming Wu, 'A Comparative Analysis of Personal Data Protection Regulations between the EU and China' (2020) 20 *Electronic Commerce Research* 565.

protection.[13] Chinese scholars have generally believed that specialized legislation can enhance the protection of personal data in China.[14] However, some have been concerned about the 'informed consent' approach adopted by the law because it may be abused by data handlers to use standard form contracts to restrict data subjects' rights or to distribute data security risks unfairly.[15] Empirical research in other jurisdictions where comprehensive data protection laws have been established has raised concerns about the efficacy of legal instruments in enhancing consumers' control over personal data.[16] Scholars have found that even though specialized legislation exerts a meaningful impact on firms' practices of contracting for personal data, two main issues need particular attention: marked differences in terms of compliance revealed through firms' ways of drafting privacy policies and incredible complexity of the privacy policies.[17] As some scholars have observed, the detail and specificity of data protection clauses between firms vary significantly, and 'many are in a state of flux'.[18] Thus, individuals may have difficulty claiming their contractual rights because of the following factors. First, individuals may be unable to determine the application of particular terms in privacy policies. Second, internet companies rarely specify how they collect, process and protect personal data in their privacy policies. Third, terms in privacy policies are constantly changing.[19] In addition, a growing number of empirical studies have demonstrated that consumers' inattentiveness to contracts would lead to them being worse off.[20]

Do Chinese firms draft their privacy policies and terms of service the same way as firms in jurisdictions with more comprehensive data protection laws? How do Chinese firms draft contracts to assign each party's rights and obligations pertaining to collecting, processing, sharing, and protecting personal information? To what extent the newly promulgated PIPL will affect the way Chinese firms contract for personal information? This paper aims to answer these questions by analysing a sample of privacy policies and terms of service. The contribution of this paper is twofold: first, it provides empirical data for

[13]Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21 *Vanderbilt Journal of Entertainment and Technology Law* 549; Shen Zhang, 'Protection of Cross-Border Data Flows Under International Investment Law' in Julien Chaisse, Leïla Choukroune, and Sufian Jusoh (eds), *Handbook of International Investment Law and Policy* (Springer, 2021).

[14]See, e.g. Liming Wang and Xiaodong Ding, 'On the Highlights, Characteristics and Application of Personal Information Law (论《个人信息保护法》的亮点、特色与适用)' (2021) 6 *The Jurist (*法学家*)* 1; Xiaodong Ding, 'Rethinking the Personal Information Protection Law from a Comparative Law Perspective: China's Path and Principle of Interpretation (《个人信息保护法》的比较法重思：中国道路与解释原理)' (2022) 25 *ECUPL Journal (*华东政法大学学报*)* 73.

[15]See, e.g. Xinbao Zhang, 'Collection of Personal Information: Restricting the Application of the Principle of Informed Consent (个人信息收集: 告知同意原则适用的限制)' (2019) 6 *Journal of Comparative Law (*比较法研究*)* 1; Ye Tian, 'The Dilemma of the Principle of Informed Consent in the Era of Big Data and the Solution (大数据时代知情同意原则的困境与出路)' (2019) 6 *Law and Social Development (*法制与社会发展*)* 111.

[16]See Oren Bar-Gill and Omri Ben-Shahar, 'Regulatory Techniques in Consumer Protection: A Critique of European Consumer Contract Law' (2013) 50 *Common Market Law Review* 109; Iris van Ooijen and Helena U Vrabec, 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective' (2019) 42 *Journal of Consumer Policy* 91.

[17]Dimitra Kamarinou, Christopher Millard and W Kuan Hon, 'Cloud Privacy: An Empirical Study of 20 Cloud Providers' Terms and Privacy Policies–Part II' (2016) 6 *International Data Privacy Law* 170, 187; Kevin E Davis and Florencia Marotta-Wurgler, 'Contracting for Personal Data' (2019) 94 *New York University Law Review* 662, 697–9.

[18]Kamarinou, Millard and Hon (n 17) 187.

[19]Ibid 186–9.

[20]See, e.g. Ian Ayres and Alan Schwartz, 'The No-Reading Problem in Consumer Contract Law' (2014) 66 *Stanford Law Review* 545; Yannis Bakos, Florencia Marotta-Wurgler and David R Trossen, 'Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts' (2014) 43 *Journal of Empirical Legal Studies* 1; Jonathan A Obar and Anne Oeldorf-Hirsch, 'The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services' (2020) 23 *Information, Communication & Society* 128.

discussing the impact of China's newly promulgated PIPL. Second, it adds some empirical findings of Chinese firms' contracting practices for personal information to the existing empirical research on the role of data-related legislation in personal data protection.

This paper uses Chinese peer-to-peer lending platforms (P2Ps) as a case study because they collect and process a significant quantity of personal information by their nature. The timeliness of this paper could be questioned because the Chinese government planned to shut down all P2Ps by mid-November 2020.[21] However, the following reasons make this paper still valuable. Firstly, this paper has practical implications for the ongoing debates over the desirability of China's PIPL regarding platforms' liability.[22] It goes beyond the findings in the P2P sector to discuss a common phenomenon among Chinese data handlers in the era of the digital economy. Secondly, although most P2Ps stopped loan-matching services, the ones in this sample maintained their websites available to allow for user registration. Some had updated their privacy policies after mid-November 2020.[23]

Based on a unique set of terms of service and privacy policies collected between June 2020 and February 2021 from 202 Chinese P2Ps, this paper investigates online contracting for personal information in China. It outlines three key issues that can be found not only in the P2P sector but in other areas of the Chinese digital industry as well. First, the lack of accessibility to privacy policies makes it difficult for individuals to find out how their personal information will be processed and protected. Second, differences in contractual terms regarding the types of personal information collected; the processing, sharing, and protection of that information; the rights of data subjects; and the resolution of disputes are notable, making them practically incomparable. Finally, the contractual terms are drafted in favour of online service providers because they are self-granting and waive their responsibility for any losses caused by data breaches. The paper further discusses whether the PIPL can help address three critical issues considered in the survey results. It argues that although the enacted law appears to be promising, its effectiveness depends upon how it is enforced in practice and how consumers respond to changes in the way that firms contract for personal information. As a result, more empirical studies are required to evaluate the effectiveness of China's personal information protection legislation.

The remainder of this paper is structured as follows. Section II illustrates provisions related to contracting for personal information in China before the promulgation of the PIPL. Section III describes the sample of hand-collected terms of service and privacy policies and the methodology used for content analysis. Section IV analyses the key issues found based on detailed survey results of the terms and privacy policies. Section V discusses whether the PIPL can address the key issues, and Section VI expounds on the conclusions.

[21] Chong Koh Ping and Xie Yu, 'China Hails Victory in Crackdown on Peer-to-Peer Lending' *The Wall Street Journal* (9 December 2020) <https://www.wsj.com/articles/china-hails-victory-in-crackdown-on-peer-to-peer-lending-11607515547> accessed 1 April 2022.

[22] Xiaohui Liang, Su Zhang and Jingze Li, 'The Second Review of the Draft Personal Information Protection Law Emphasizes the Supervision of "Giant Internet Platforms"' (www.chinanews.com, 26 April 2021) <https://www.chinanews.com.cn/gn/2021/04-26/9464400.shtml> accessed 1 April 2022.

[23] According to other news reports, all P2Ps were to close in April 2021. See Jie Cheng, 'POBC: All P2Ps In Operation Closed Down' *Xinhuanet* (16 April 2021) <http://www.xinhuanet.com/fortune/2021-04/16/c_1127335851.htm> accessed 1 April 2022.

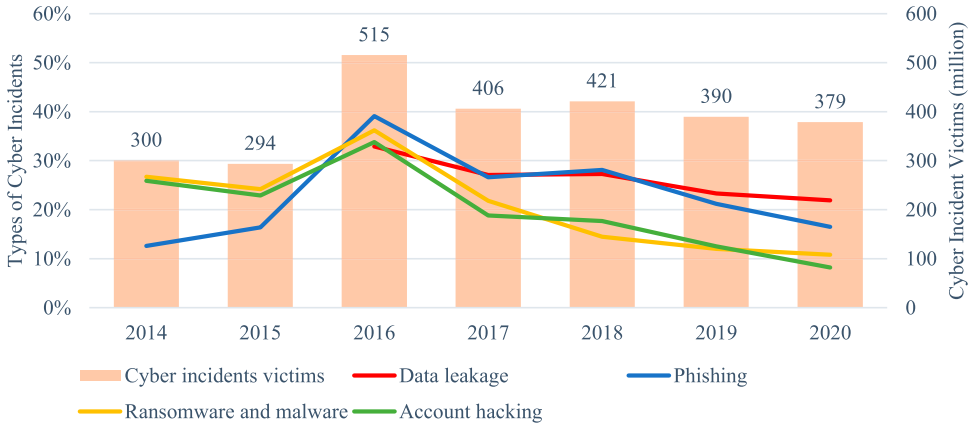

Figure 1. Number of cyber incident victims and causes in China, 2014–2020. Source: Data derived from China Internet Network Information Centre reports.

II. PROVISIONS RELATED TO CONTRACTING FOR PERSONAL INFORMATION IN CHINA BEFORE THE PIPL

China's digital industry possesses great potential, but its development has been described as being in a 'wild era'.[24] The weak protection of personal information and inadequate attention paid by Chinese netizens to personal information have led to the production of numerous online and telephone scams and the abuse of such personal information.[25] Figure 1 shows the number of victims of cyber incidents and the nature of their causes from 2014 to 2020. On average, there were 386 million Chinese netizens who experienced internet incidents annually. The main types of cyber incidents changed during this period. Before 2016, ransomware, malware, and account hacking were among the most common cyber incidents. From 2016 onward, the most common cyber incidents were data leaks and phishing. Data leaks have overtaken phishing as the most frequently reported cyber incident since 2019. Approximately 21.9 per cent of Chinese netizens reported that their personal information was exposed in 2020.[26]

Against this backdrop, China's data protection legislation has undergone significant changes over the past few years.[27] Lawmakers have been increasingly focused on the protection of personal information rather than cybersecurity.[28] Nevertheless, before the promulgation of the PIPL in 2021, China's legal framework for protecting personal

[24]Celia Chen, 'China's 'Wild Era' of Internet May Be Ending as New Personal Data Protection Law Seeks to Curb Big Tech's Control Over User Data' *South China Morning Post* (26 November 2020) <https://www.scmp.com/tech/policy/article/3111337/chinas-wild-era-internet-may-be-ending-new-personal-data-protection-law> accessed 11 January 2021.
[25]Adam Minter, 'Why China Doesn't Care About Privacy' *Bloomberg* (17 May 2016) <https://www.bloomberg.com/opinion/articles/2016-05-17/why-china-doesn-t-care-about-privacy> accessed 21 January 21.
[26]CINIC (n 2) 85.
[27]The legal blueprint for personal data protection was mapped out in the Chinese government's 'National Big Data Strategy (国家大数据战略)' in 2016. See Outline of the 13th Five-Year Plan for the National Economic and Social Development of the People's Republic of China (中华人民共和国国民经济和社会发展第十三个五年规划纲要) (issued by the NPC on 16 March 2016, effective on 16 March 2016), ch 28.
[28]See, e.g. Jon R Lindsay, Tai Ming Cheung and Derek S Reveron (eds), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (OUP, 2015); Greg Austin, *Cybersecurity in China: The Next Wave* (Springer, 2018).

Table 1. Provisions related to contracting for personal information before the promulgation of the PIPL.

	Provisions
General principle	principles of legality, propriety, and necessity
	consent requirements
Format	explicit statements
Content	rules for collection and use of personal information
	purposes, means, and scope for collecting or using information
	right to delete or correct personal information
	methods for making complaints or reports

information was fragmented. No specialized law existed, and relevant provisions were scattered among general laws, departmental rules, guidelines, and notices.[29] For the purpose of this study, the following analysis of provisions mainly focuses on those related to contracting for personal information in laws and regulations before the promulgation of the PIPL (see Table 1).

In general, the provisions on contracting for personal information exhibit two characteristics. First, the related provisions are too principled. Online service providers must adhere to 'the principles of legality, propriety, and necessity' when collecting, processing, sharing, and disclosing users' personal information.[30] They must obtain individual consent before collecting and processing personal information unless there are exceptions prescribed by laws and regulations elsewhere.[31] When obtaining an individual's consent, online service providers must disclose their purposes, means and scope in relation to the collection and processing of personal information.[32] Online services providers must not collect personal information unrelated to their services. Also, they must not process any personal information in violation of the relevant laws or regulations or the agreements they have entered into.[33] They cannot share or release any personal information unless it has been approved by the user or anonymized.[34] However, there are no specific requirements for disclosure methods.

Second, the related provisions are less concerned with the rights of data subjects. Online service providers are required to provide individuals with certain rights regarding their personal information. Even though the Cybersecurity Law does not expressly mention the rights of the data subject, the spirit of the right to be forgotten can be seen in the provision that provides individuals with the right to request the correction or deletion of personal information.[35] In addition, online service providers are also required to establish a proper complaint and reporting system for individuals to complain about matters related to the security of their personal information. They shall inform individuals of the methods and procedures for submitting complaints and respond to individuals' inquiries in a timely manner.[36] Furthermore, online service providers are encouraged

[29]See Appendix I for a detailed list of data-related laws, departmental rules, guidelines and notices.
[30]Cybersecurity Law (n 6), Art. 41(1).
[31]Ibid, Art. 22(3).
[32]Ibid, Arts. 22(3) and 41(1).
[33]Ibid, Art. 41(2); Civil Code (n 9), Art. 1035.
[34]Cybersecurity Law (n 6), Art. 42(1).
[35]Ibid, Art. 43.
[36]Ibid, Art. 49(1).

to conduct regular risk assessments to identify potential hazards and strengthen the security of their network services.[37]

III. SAMPLE AND METHODOLOGY

A. Sample of terms of service and privacy policies

Upon collection, the study reviews the standard terms of service and privacy policies available during the sign-up process on the P2Ps' websites.[38] The sample collection was undertaken between June 2020 and February 2021, before the passage of the PIPL. A two-step manual procedure was used to construct the sample. Firstly, a list of P2Ps was developed using information available on Wang Dai Zhi Jia (*Home of Online Lending*), a website that was used to update P2Ps' information. The information obtained from the website was considered reliable because of the website's frequent use as the source of data in many studies and policy recommendations regarding China's P2P lending.[39] Secondly, the terms of service and privacy policies of each P2P's website were reviewed. In the case of P2Ps with privacy policies, the terms of service were collected and examined to determine whether they incorporated, complemented, or conflicted with the privacy policies. The present study did not examine other legal documents, such as cookie policies, risk disclosure statements, assignment of credit agreements, and loan intermediary service agreements. The reason is that the study focuses on contracting for personal information rather than the overall service offered by online service providers.[40]

A total of 277 contractual documents (75 privacy policies and 202 terms of service) were collected from 202 P2Ps. This study collected information about P2Ps, such as business period, registered industry, type, and location of headquarters.[41] This study also gathered information on whether P2Ps received government investment or external funding.[42] All information was obtained from the National Enterprise Credit Information

[37]Ibid, Arts. 17 and 29.

[38]P2Ps differ significantly in how they present data protection clauses. The first approach is providing a privacy policy for users to read during their registration process. Users must click 'I agree' before moving to the next registration step; otherwise, they cannot complete the registration process. The second approach is that a privacy policy is not available for users to read during their registration process. However, rules regarding personal data protection can be found somewhere on the P2P's website, usually presented as a privacy statement. The third approach is that clauses regarding personal data collection, use and protection can be found in a P2P's terms of service.

[39]See, e.g. Wei Shen, 'Designing Optimal Regulation for Financial Innovation in Capital Raising – Regulatory Options for China's Peer-to-Peer Lending Sector' (2016) 31(3) *Banking & Finance Law Review* 539–72; Chuanman You, 'Recent Development of FinTech Regulation in China: A Focus on the New Regulatory Regime for the P2P Lending (Loan-based Crowdfunding) Market' (2018) 13(1) *Capital Markets Law Journal* 85–115; Robin Hui Huang, 'Online P2P Lending and Regulatory Responses in China: Opportunities and Challenges'(2018) 19 *European Business Organisation Law Review* 63–92.

[40]Existing empirical studies generally exclude the FQAs or cookie policies which may contain data-related provisions. See Christopher Millard (ed), *Cloud Computing Law* (OUP, 2013).

[41]The business period is defined as 2020 minus the year of founding. State shareholding means state shares plus state-owned enterprises shares of a P2P. I construct the dummy variable for type, registered industry, region and IFA member. Dummy variable Type, which is equivalent to one if a P2P is registered as a limited-liability company and zero otherwise. Dummy variable Registered Industry, which is equal to one if a P2P's registered industry is financial-related (i.e. finance, financial services, capital market services) and zero otherwise. Dummy variable Region, which is equivalent to one if a P2P is registered in the eastern part of China and zero otherwise. Dummy variable NIFA member, which is equivalent to one if a P2P is a member of the National Internet Finance Association of China and zero otherwise.

[42]I also construct the dummy variable for state shareholding and external funding. Dummy variable State shareholding, which is equivalent to one if a P2P has at least one government-related shareholder (i.e. central or local government,

Table 2. Characteristics of P2Ps in the sample ($n = 202$).

Characteristics	Mean	Median	S.D.	Min	Max	*N*
Business period (years)	5.82	6.00	1.31	2	10	202
Registered capital (RMB)	202,925,313	50,040,000	408,262,072	5,000,000	3,158,044,667	202
Type	0.93	1	0.26	0	1	202
Registered industry	0.34	0	0.47	0	1	202
State shareholding (%)	20.17	0	35.15	0	100	202
External funding	0.37	0	0.48	0	1	202
Region	0.82	1	0.38	0	1	202
NIFA member	0.26	0	0.44	0	1	202

Publicity System, an online search engine that allows the public to access official records of registered Chinese companies.[43]

Table 2 summarizes the characteristics of the P2Ps in the sample. P2Ps operate for an average of six years, with the shortest period being two years and the longest being ten years. The size of P2Ps varies greatly. Their registered capital ranges from RMB 5 million to RMB 3.1 billion, with a mean of RMB 202.9 million. Most P2Ps in the sample are based in the eastern part of China (82 per cent) and registered as limited-liability companies (93 per cent). Despite this, only 34 per cent of sample P2Ps are registered to provide financial services. Even fewer (26 per cent) are members of National Internet Finance Association of China (NIFA). State shareholding accounts for approximately 20 per cent of shares of P2Ps, indicating that the Chinese government and government-related companies play a role in the sector.

B. Categorizing information provisions in terms of service and privacy policies

Using a case study approach, this paper explores how online service providers incorporate personal information protection obligations into their terms of service and privacy policies in China. These contractual documents contain terms that pertain to the collection, processing and sharing of personal information, the rights of data subjects, the obligations of data handlers, and dispute resolution in cases of a data breach. Different approaches have been used to categorize personal data protection terms in previous studies. For example, Kamarinou, Milard and Hon group clould providers' privacy-related terms into three main categories: transparency provisions; data subjects' rights and data security; and legal framework for potential remedies.[44] Davis and Marotta-Wurgler divide privacy policies into ten categories, including contextual integrity, data accuracy safeguards, data breach, data retention practices, notice, privacy by design, processor contracts, security measures, sharing consent, and user control.[45] For the purpose of this study, the terms were grouped into five broad categories, loosely based on a non-binding national standard known as the Personal Information Security Specification.[46]

state-owned enterprises) and zero otherwise. Dummy variable External funding, which is equivalent to one if a P2P has received external funding (eg, angel investor funding, series A, B, C, D, E funding) and zero otherwise.

[43]Official website at http://www.gsxt.gov.cn/index.html.

[44]Dimitra Kamarinou, Christopher Millard and W Kuan Hon, 'Cloud Privacy: An Empirical Study of 20 Cloud Providers' Terms and Privacy Policies–Part I' (2016) 6 *International Data Privacy Law* 79, 82–3.

[45]Davis and Marotta-Wurgler (n 17) 697–9.

- The first category, Personal Information Collection and Use, contains terms that define personal information, the methods to collect it, and the purpose of using it.
- The second category, Personal Information Sharing, includes terms describing situations where personal information handlers share information with related stakeholders.
- The third category, Rights of Data Subjects, contains terms illustrating data subjects' right to access, correct and erasure, and their right to withdraw consent on personal information collection or sharing.
- The fourth category, Data Security, comprises terms that govern data controllers and processers' obligation to secure personal data and situations wherein they waive their liability.
- The fifth category, Dispute Resolution, includes terms about the choice of dispute resolution methods.

IV. THE CORE FINDINGS

These findings concern how online service providers incorporated prescribed provisions regarding personal information protection into their contracts. Even though these findings are derived from a case study of the P2P sector, the three key issues, namely, the 'issue of accessibility and readability', the 'issue of variation' and the 'issue of one-sided terms', are generally observed in online contracting for personal information in China.

A. The issue of accessibility and readability of privacy policies

Online service providers are expected to offer privacy policies that specify the parties' rights and obligations related to collect, process, share, and protect personal information. However, the findings indicate some serious issues regarding the accessibility and readability of privacy policies.

More than half of the sample P2Ps (62.87 per cent) do not provide privacy policies during the sign-up process on their websites. Table 3 compares the characteristics of P2Ps with and without privacy policies. The last column reports the difference in mean (T-Test results for continuous variables and Pearson Chi-Square results for binary variables). Compared to those without privacy policies, P2Ps with privacy policies are larger, are more concentrated in the eastern part of China, and are more likely to have a membership in NIFA. P2Ps with privacy policies are also more likely to retain their business status and receive government-related investment than those without privacy policies.

[46]Information Security Technology – Personal Information Security Specification (GB/T 35273–2017) (信息安全技术——个人信息安全规范) (issued by the General Administration of Quality Supervision, Inspection and Quarantine and Standardization Administration of China (SAC) on 29 December 2017, effective on 1 May 2018). The revised version (GB/T 35273–2020) was issued by the State Administration for Market Regulation and the SAC on 6 March 202, effective 1 October 2020 (hereinafter 'Personal Information Security Specification'). It is a non-binding national standard that perform a key implementing role to Cybersecurity Law in respect of personal information protection before the promulgation of the PIPL.

Table 3. Availability rate of privacy policies among P2Ps.

	With privacy policies		Without privacy policies			
Characteristics	Mean	S.D.	Mean	S.D.	Diff. in Mean	Pearson Chi-Squared
Business period	6.00	1.56	5.71	1.13	1.534	
Registered capital (Log10)	8.00	0.61	7.79	0.51	2.716***	
Type	0.93	0.25	0.92	0.27		0.100
Registered industry	0.37	0.49	0.31	0.47		0.719
State shareholding (%)	26.25	39.72	16.57	31.77	1.798**	
External funding	0.40	0.49	0.35	0.48		0.421
Region	0.91	0.29	0.77	0.42		5.869**
NIFA member	0.39	0.49	0.18	0.39		10.424***
Number of Observations	75		127			

Note: * $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

Table 4. Times to read P2Ps' terms of service and privacy policies for average readers.

	Number	Max	Min	Mean	Avg. Reading time (260 characters/min)[a]
Terms of Service	202	16102	1854	8392	≈32 minutes
Privacy Police	75	17003	1651	7908	≈30 minutes

[a]It was found that the Chinese's reading speed was around 259.5 ± 38.2 Chinese characters per minute. See Chen-Xiao Wang, Na Lin and Ying-Xuan Guo, 'Visual Requirement for Chinese Reading with Normal Vision' (2019) 9 Brain and Behavior e01216.

Furthermore, the terms of service and privacy policies offered by P2Ps may require individuals to spend considerable time reading. Table 4 shows the word count and reading time of terms of service and privacy policies. Both contractual documents vary significantly in length. The longest privacy policy has 17003 Chinese characters, whereas the shortest one has only 1651 Chinese characters. On average, a privacy policy has 7908 Chinese characters, taking approximately 30 minutes to read. If no privacy policies are provided, users may have to spend a little more time searching for relevant information in terms of service. In general, reading terms of service takes users 32 minutes on average. The finding supports the existing conclusion that consumers spend an inordinate amount of time searching for relevant information due to long and complex standard form contracts.[47]

The accessibility and readability of privacy policies raise concerns about the extent to which individuals have been fully informed about the collection, processing and protection of personal information when registering for network services. As mentioned, the low accessibility rate of privacy policies suggests that individuals may have difficulty obtaining helpful information regarding the collection, use, and protection of personal information. Even if privacy policies are readily accessible, individuals will not likely read them because standard-form contracts have not been written in a way that encourages reading.[48]

[47]See Ayres and Schwartz (n 20); Mitu Gulati and Robert E Scott, *The Three and a Half Minute Transaction: Boilerplate and the Limits of Contract Design* (The University of Chicago Press, 2012); Adam S Chilton and GalitSarfaty, 'The Limitations of Supply Chain Disclosure Regimes' (2017) 53 *Stanford Journal of International Law* 1.

[48]See generally, Ayres and Schwartz (n 20). There are other reasons: consumers are more focused on the products or services, and unaware of the contract terms. See Sandra Booysen, 'Singapore' in Sandra Booysen and Dora Neo (eds), *Can Banks Still Keep a Secret? Bank Secrecy in Financial Centres around the World* (CUP, 2017).

B. The issue of variation in terms of service and privacy policies

Following the assessment of the accessibility and readability of privacy policies, this part presents the content analysis results of the terms of service and privacy policies. The results conclude that significant variations exist in contract terms relating to the types of personal information collected; information processing, sharing, and protection; the rights of data subjects; and dispute resolution.

1. Various types of personal information collected by P2Ps

Under the Cybersecurity Law, personal information refers to any information relating to an identified or identifiable natural person, including a person's name, identification number, an online identifier and socioeconomic status.[49] Although the law restricts online services providers from over-collecting personal information, the results indicate they often extend the scope of personal information to link to or combine other non-personally identifiable information.[50]

As shown in Figure 2, P2Ps can collect various types of personal information, as specified in their terms of service and privacy policies. Some types of personal information are more likely to be collected by P2P than others. The types of information most likely to be collected are those that are necessary for registering an account. Such information includes user contact details (81.68 per cent), user background (81.19 per cent) and personal identification (78.71 per cent). Furthermore, financial information related to the user's assets and credit is also likely to be collected because of the nature of P2P lending. The information, including users' salary, financial asset status and personal credit history reports, is collected in order to know users and match them with suitable loans. By contrast, information, such as the location of users and their biometric information, is less likely to be collected.

The study also observes the distinction between sensitive and non-sensitive personal information of the sort that affects the extent of protection to be provided by data handlers. Based on Table 5, a majority (75.25 per cent) of the P2Ps in the sample do not distinguish sensitive personal information from non-sensitive information. Only a small percentage (17.33 per cent) of P2Ps define sensitive personal information and further elaborate on its scope. Thefindings can be explained by the fact that such distinctions had not been prescribed by any laws or regulations before the promulgation of the PIPL.[51]

Furthermore, the results indicate that P2Ps collect personal information from users directly and from other sources, such as news reports, government information disclosures, court judgments and credit agencies. According to their terms of service and privacy policies, personal information is collected for three purposes: to meet statutory requirements,[52] to provide better and safer service and for marketing purposes.

[49]Cybersecurity Law (n 6), Art. 76(5).

[50]Kamarinou, Millard and Hon (n 44) 84–5. For a detailed discussion about the meaning of the broad concept of personal data, see Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) *Law, Innovation and Technology* 40.

[51]A non-binding national standard defines sensitive personal information. See Personal Information Security Specification (n 46), para 3.1–3.2.

[52]P2Ps are mandated to perform anti-money laundering and anti-terrorist financing obligations following the laws in China. They are also required to collect users' personal information to meet the requirements of real-name registration and mandatory information disclosure requirements. See Decision on Strengthening Information Protection on Networks (关于加强网络信息保护的决定)(promulgated by the SCNPC on 28 December 2012, effective 28 December

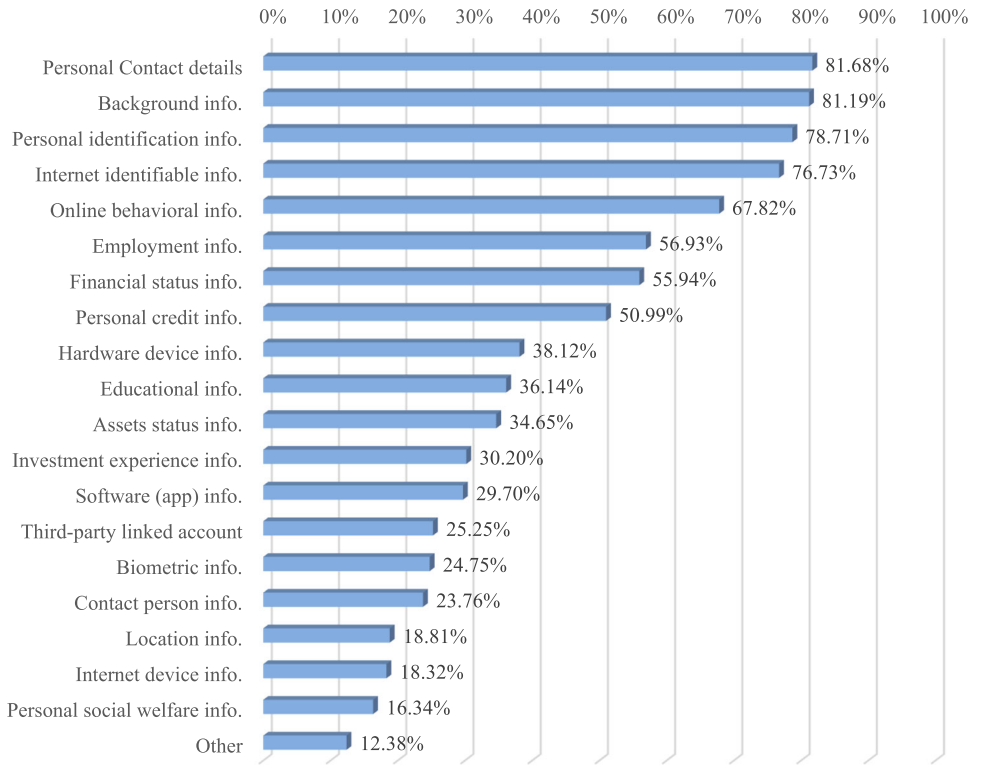

Figure 2. Types of personal information collected by P2Ps.[53]

Note: For the specific personal information contained in each category, see Appendix 2.

Table 5. Number of P2Ps that distinguish sensitive and non-sensitive personal information.

	Frequency	% of 202
Sensitive personal information are not defined.	152	75.25%
List some sensitive personal information as examples.	15	7.43%
Define and elaborate sensitive personal information.	35	17.33%

Nevertheless, consistent with findings elsewhere, P2Ps generally make the list of purposes not exhaustive, leaving space to expand personal data collection scope.[54]

2. Personal information shared among various entities

As revealed by the survey results, P2Ps share personal information with various entities. Sharing personal information is claimed to comply with relevant laws and regulations

2012), Art. 6; Guidelines for the Disclosure of Information on the Business Activities of Online Lending Information Intermediary Institutions (网络借贷信息中介机构业务活动信息披露指引) (promulgated by the China Banking Regulatory Commission (CBRC) on 23 August 2017, effective 23 August 2017), Arts. 2 and 9(7); Anti-Money Laundering Law of the People's Republic of China (中华人民共和国反洗钱法) (promulgated by the SCNPC on 31 October 2006, effective 1 January 2007), Arts. 3 and 18; Cybersecurity Law (n 6), Art. 24.

[53]Some P2Ps in the sample only outline the collection of personal information, but does not specify the types of personal information.

[54]See Kamarinou, Millard and Hon (n 44) 92–3.

or provide better service. This paper classifies the patterns of sharing personal information into two types based on the characteristics of the data recipients: 'horizontal sharing' and 'vertical sharing'.

'Horizontal sharing' refers to sharing personal information between members of equal standing. Online service providers must obtain users' consent before sharing personal information with their subsidiaries, partners and third-party service providers. 'Vertical sharing' refers to sharing personal information between members, where one party has greater power or authority over the other. Online service providers often notify users that they can share, transfer or disclose personal information to relevant authorities or stakeholders in given situations. These situations include satisfying the real-name registration requirements, the necessity for national security, public interests and law enforcement.

This distinction between 'horizontal sharing' and 'vertical sharing' is critical because it establishes the data handlers' obligation to obtain the user's consent before sharing personal information horizontally. Nevertheless, the results of this study indicate that P2Ps generally do meet the requirements for data sharing, thereby posing the risk of unreasonably sharing personal information. Users may also encounter problems if they refuse to allow their personal information to be shared, such as having their account registrations denied or suffering interruptions when using the service.

Furthermore, most P2Ps in the sample include an exception clause stating that according to relevant laws and regulations, they can share, transfer and disclose personal information without obtaining the consent of users under the following circumstances:

- when related directly to the fulfilment of obligations stipulated by laws and regulations;
- when related directly to homeland security and national defence;
- when related directly to public safety, public health and other significant public interests;
- when related directly to a criminal investigation, prosecution, trial and judgment enforcement;
- when safeguarding the primary lawful rights and interests, such as life and personal property, but having difficulty obtaining users' consent;
- when disclosing personal information voluntarily to the general public;
- when personal information is collected from legitimate public information sources, such as news reports and open government information; and
- when required by authorities with the good-faith belief that disclosure of personal information is reasonably necessary.[55]

Thus, personal information will likely be shared extensively between P2Ps and the various stakeholders, raising serious concerns because, in many cases, users are not informed that their personal information is being shared or disclosed. The users' right to withdraw consent or authorization for sharing personal information is symbolic because of the potential interruption caused by exercising such a right.

[55]See, e.g. privacy policies from Renren Dai and Yiren Wealth, and others. Similar content can be found in para 5.6 of the Personal Information Security Specification (n 46).

C. The issue of one-sided contract terms

To protect personal information, appropriately designing the rights-and-remedies scheme is critical.[56] However, studies have shown that standard form contracts are often designed in favour of sellers, particularly in contract terms related to buyer rights, liability waivers and dispute resolution.[57] Thus, this part analyses these three categories of terms to illuminate the issue of one-sided contract terms in online contracting for personal information.

1. Limited rights towards personal information

The issue of one-sided contract terms first manifests itself in the situation that P2Ps provide users with limited control over their personal information. As shown in Table 6, a majority (about 61 per cent) of surveyed P2Ps do not provide users with rights related to their personal information. If such rights are provided, they are more likely to be mentioned in the privacy policies than in terms of service. Therefore, it is reasonable to expect that the mandatory adoption of privacy policies by data handlers will result in a significant improvement in the protection of personal information. Furthermore, the scope of data subjects' rights varies among P2Ps offering such rights. Users are more likely to have the right to access (32 per cent) and correct (28 per cent) personal information over the right to object (20 per cent) and delete (21 per cent).

In light of the survey results, the rights of data subjects have not been adequately valued and protected. Such a phenomenon can be explained to some extent by the fact that data subjects' rights were not explicitly prescribed in any laws and regulations before the PIPL.[58] Restrictions may be expected even if P2Ps provide rights to data subjects. Some examples include situations relating to national security, public interest and law enforcement. Others include data subjects abusing their rights or acting maliciously by exercising data rights in a way that causes severe injury or property damage to others or by disclosing trade secrets.[59]

2. Unclear time limit for the retention of personal information

The issue of one-sided contract terms is also reflected in the unclear time limit for retaining users' personal information. The results also suggest that P2Ps may not cease to retain personal information once the purpose for which it was collected is no longer being served or when retention is no longer necessary for legal or business purposes. As shown in Table 7, a majority (about 70 per cent) of P2Ps in the sample do not specify the data retention period. Approximately 14 per cent of P2Ps inform users that they will keep their personal information within the legally required period, which can vary according to the laws and regulations in China.[60] Only a small portion of the surveyed

[56] Jacob M Victor, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy' (2013) 123 *Yale Law Journal* 513, 515.

[57] See, e.g. Florencia Marotta-Wurgler, 'What's in a Standard Form Contract? An Empirical Analysis of Software License Agreements' (2007) 4 *Journal of Empirical Legal Studies* 677; Qin Zhou and Jing Feng, 'What We Do and Do Not Know About Standard Form Contracts? An Empirical Study of Wealth Management Product Contracts in China' (2021) 16 *Asian Journal of Comparative Law* 124.

[58] Chapter 4 of the PIPL prescribes the rights of data subjects.

[59] See, e.g. Lufax Privacy Policy and others.

[60] See Cybersecurity Law (n 6), Art. 21(3) requires network operators to monitor and record network operation status and network security incidents and maintain relevant network logs for no less than six months. However, the E-commerce

Table 6. P2Ps' approach to rights of data subjects.

	Mentioned in privacy policies ($n = 75$)		Mentioned in terms of services ($n = 127$)		Total ($n = 202$)	
	Frequency	%	Frequency	%	Frequency	%
Right to access	54	72.00	10	7.87	64	31.68
Right to retification	54	72.00	3	2.36	57	28.22
Right to object	37	49.33	3	2.36	40	19.80
Right to delete	38	50.67	4	3.15	42	20.79
Overall	58	77.03	13	1.75	71	38.61

Table 7. P2Ps'approaches to data retention period.

	Frequency	% of 202
Up to 1 month (or 30 days) after closing the account	13	6.4%
No less than 5 years after closing the account	20	9.9%
A retention period required by law	28	13.9%
Unknown	141	69.8%

P2Ps have a specific personal information retention period. Approximately 10 per cent specify that personal information will be kept for at least five years, which is the minimum time for which P2Ps must retain users' weblogs and transaction information after the end of their loan contracts.[61] Another six per cent P2Ps are in the sample that explicitly states that personal information will be retained for one month (or 30 days).

Given the uncertain period for data retention, P2Ps must take measures to safeguard the integrity and confidentiality of personal information. Encryption and anonymization are means of securing personal information that most P2Ps mention. Personal information will be encrypted and stored on P2Ps' servers, and data access rights will be strictly controlled during data transmission using the encrypted transmission protocol. Furthermore, P2Ps will anonymize personal information before performing statistical analyses. Such anonymized information will be stored separately from the information used to identify users. Nevertheless, the implementation and effectiveness of these measures are unknown.

3. Abuse of disclaimer

The issue of one-sided contract terms is further highlighted by the approaches P2Ps take when distributing responsibilities in the event of data leaks or damage. P2Ps in the sample employ three tactics to avoid their liabilities: expanding the scope of force majeure, excluding technical failure from liability and setting a liability cap, as shown in Figure 3.

Approximately 35 per cent of sample P2Ps expand the definition of force majeure[62] to include financial market volatility, hacker attacks, computer viruses and system defects, in

Law of the People's Republic of China (中华人民共和国电子商务法) (promulgated by the SCNPC on 31 August 2018, effective on 1 January 2019), Art. 31 requires e-commerce businesses to store product and service information and transaction information no less than three years from the date of completing the transaction.

[61] See Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions (网络借贷信息中介机构业务活动管理暂行办法)(promulgated by the CBRC and others on 17 August 2016, effective on 17 August 2016), Art. 18(2); Guidelines on the Depository Business for Funds of Online Peer-to-Peer Lending (网络借贷资金存管业务指引) (promulgated by the CBRC on 23 February 2017, effective on 23 February 2017), Art. 9 (4).

[62] Civil Code (n 9), Art. 180(2) refers to force majeure to any objective circumstance that is unforeseeable, inevitable and insurmountable. Chinese scholars provide three interpretations in defining force majeure: 'objective', 'subjective' and

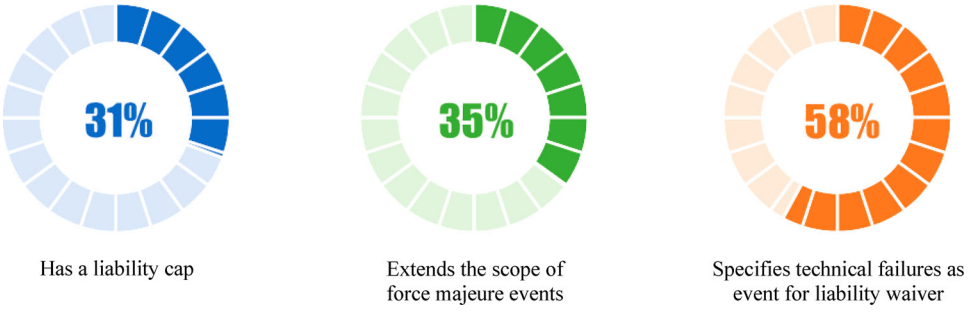

Figure 3. P2Ps' approaches to liability waivers.

addition to events commonly recognized as force majeure such as war, strikes, legislative and administrative interference, accidental technology failures and natural disasters.[63] The extension of the scope of force majeure events allows P2Ps to claim reduction or exemption of contractual liability in numerous situations.[64] Nearly 58 per cent of sample P2Ps indicate that they are not responsible for technical issues, such as system maintenance, interruptions caused by hacker attacks, technology upgrades or malfunctions of the network infrastructure. Furthermore, about 31 per cent of the sample P2Ps claim that liability for losses is subject to a financial cap not exceeding the fee received from the user. Thus, if a user does not pay any service fees at the time of data leaks or damage, these P2Ps will not be liable for any monetary loss resulting from such an event.

In brief, the survey results demonstrate that P2Ps exclude their responsibility from a broader scope of events. The findings are consistent with those from previous studies that have suggested that data handlers often use waivers of liability to expand exemptions, notwithstanding those restrictions on the use of exemption and similar clauses stipulated in specialized laws.[65]

4. Restricted options for dispute resolution

The final aspect of the issue of one-sided contract terms is related to dispute resolution. The results indicate that P2Ps impose restrictions on the choice of dispute resolution mechanisms. As shown in Figure 4, nearly one quarter (23 per cent) of the P2Ps in the sample specify that arbitration is mandatory, with 13 naming the Beijing Arbitration Commission, 12 naming the Guangzhou Arbitration Commission, and 7 naming the Shenzhen Court of International Arbitration.[66] Furthermore, P2Ps in the sample also limit the choice

'compromise'. See Yi Wang, 'COVID-19, Force Majeure, and Change of Circumstance (新冠肺炎疫情、不可抗力与情势变更)' (2020) 43 *Law Science (法学)* 36, 37–8.

[63]Chinese scholars argue that judges and scholars in different jurisdictions hold different opinions about the force majeure events.See Jianyuan Cui, 'Force Majeure Clause and Its Interpretation (不可抗力条款及其解释)' (2019) 41 *Global Law Review (环球法律评论)* 48.

[64]Civil Code (n 9), Arts. 533, 563 and 590.

[65]See, e.g. Oren Bar-Gill, *Seduction by Contract: Law, Economics, and Psychology in Consumer Markets* (OUP, 2012); Daniel Schwarcz, 'Reevaluating Standardized Insurance Policies' (2011) 78 *University of Chicago Law Review* 1263; Florencia Marotta-Wurgler and Robert Taylor, 'Set in Stone: Change and Innovation in Consumer Standard-form Contracts' (2013) 88 *New York University Law Review* 240; Sandra Booysen, 'Twenty Years (and More) of Controlling Unfair Contract Terms in Singapore' (2016) *Singapore Journal of Legal Studies* 219; Lin Lin, 'Managing the Risks of Equity Crowdfunding: Lessons from China' (2017) 17 *Journal of Corporate Law Studies* 327.

[66]Other arbitration centres include China International Economic and Trade Arbitration Commission and the arbitration commission in Shanghai, Wuhan, Chongqing, Qingdao and Guiyang.

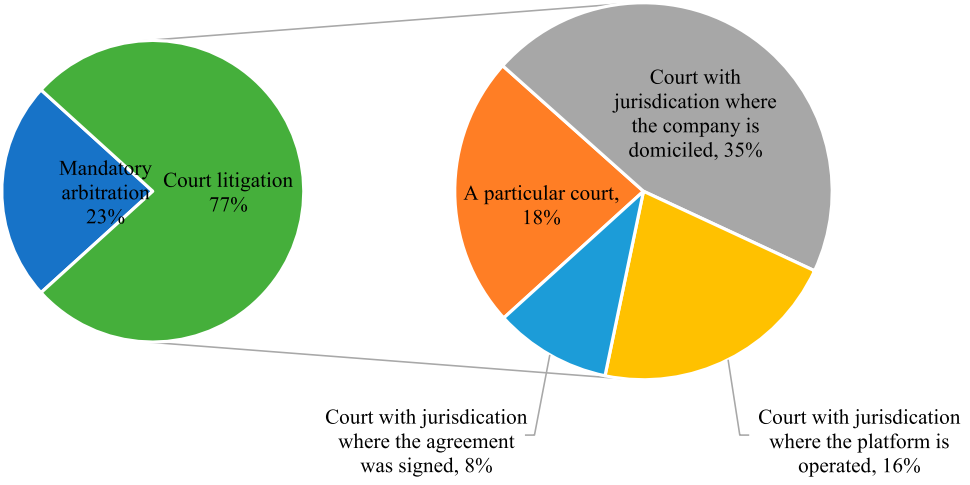

Figure 4. P2Ps' approaches to dispute resolution mechanism.

of forum. They restrict users to litigating in one of the following courts: a specific court designated by the P2P (18 per cent), the court where the company is domiciled (35 per cent), the court where the platform is operated (16 per cent) or the court where the agreement is signed (8 per cent). The cross-check results suggest that P2Ps' preference for choosing dispute resolution mechanisms may arise from their consideration of choosing the most convenient method of resolving disputes. Despite the differences in the choice of dispute resolution mechanisms and the forum selection, all of the P2Ps in the sample encourage negotiation as the primary method for dispute resolution. They also stipulate that Chinese law should govern contract validity, interpretation and execution.

To sum up, the survey results highlight three key issues concerning online contracting for personal information based on the case study of P2Ps' terms of service and privacy policies. These issues, namely, the low level of accessibility of privacy policies, significant variations in terms of service and privacy policies pertaining to the types of personal information collected and shared, and biased contract terms, highlight the insufficient protection of personal information in China. A major reason for this phenomenon can be identified in the fact that China lacked a compelling personal data protection law, and the legal framework for protecting personal data was too fragmented before the promulgation of PIPL.[67] The next section discusses how China's PIPL may affect online contracting for personal information.

V. PIPL AND THE ISSUES IN ONLINE CONTRACTING FOR PERSONAL INFORMATION

The three key issues found in this study are not limited to the P2P market. They also exist widely in China's digital market. For example, a large-scale survey of Chinese mobile

[67]See Anja Geller, 'How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective' (2020) 69 *GRUR International* 1191, 1202–3; Feng Yang and Milton L Mueller, 'Internet Governance in China: A Content Analysis' (2014) 7 *Chinese Journal of Communication* 446.

applications' data protection practices has shown that personal information is exposed to illegal acquisition and collection risks, malicious abuse and dissemination and excessive retention.[68] Similar issues have also been found in other jurisdictions where data protection regimes are more comprehensive than China's.[69] This section discusses whether the PIPL can address the three issues regarding online contracting for personal information. The paper argues that, even though the new law looks promising and may address some of the abovementioned issues, its efficacy will ultimately depend on how it is enforced in practice and how consumers respond to the firms' changes in online contracting for personal information.

A. The game-changing pIPL

China's data protection regulations are undergoing a transformation, and this area has seen considerable improvement in recent years. During the time of writing, China released two drafts of the PIPL.[70] The law ultimately took effect on 1 November 2021. It aims to achieve three objectives: protecting individuals' rights to personal information, maintaining a sound ecology of cyberspace, and stimulating the development of the digital economy.[71] As the country's first piece of legislation that contains comprehensive rules on personal information protection, the PIPL brings significant changes to personal information governance.

The PIPL integrates the fragmented personal information protection regime into a single comprehensive law. It combines and expands on personal information provisions in existing laws and regulations. As shown in Table 8, the law significantly clarifies definitions and rules. The first and most noticeable contribution of the PIPL is that it sets forth specific provisions on state organs handling personal information. State organs handling personal information shall abide by the principle of not exceeding the scope or extent necessary to fulfil their statutory duties and responsibilities.[72] They shall also fulfil notification duties.[73] Secondly, the PIPL defines 'personal information' and 'sensitive personal information' and makes a distinction between these two terms.[74] Such distinction is meaningful as the law sets forth general principles and

[68]See China Academy of Information and Communications Technology, 'White Paper on Mobile Application (App) Data Security and Personal Information Protection (2019) (移动应用(App)数据安全与个人信息保护白皮书(2019年))' (Report, December 2019) 9–17 <http://www.caict.ac.cn/kxyj/qwfb/bps/201912/P020191230332039577332.pdf> accessed 19 March 2021; '"Internet+Industry" Personal Information Protection Research Report (2020) ("互联网+行业"个人信息保护研究报告(2020年))' (Report, March 2020) 18–26 <http://www.caict.ac.cn/english/research/whitepapers/202005/P020200528474788077236.pdf> accessed 19 March 2021.

[69]Davis and Marotta-Wurgler empirically examined 194 privacy policies from firms offering online services in the United States and found that firms across online markets exhibited different compliance toward GDPR. See Davis and Marotta-Wurgler (n 17); Lisa Parker and her co-authors conducted a critical content analysis of 61 mental health apps in English-speaking markets, and concluded that the app industry paid insufficient attention to users' personal information and others. See Lisa Parker and others, 'How Private is Your Mental Health App Data? An Empirical Study of Mental Health App Privacy Policies and Practices' (2019) 64 *International Journal of Law and Psychiatry* 198.

[70]The first draft PIPL was released for public comments between 21 October 2020 and 19 November 2020. The second draft PIPL was released for public comments between 26 April 2021 and 28 May 2021.

[71]Junchen Liu, the Deputy Director of the Legal Affairs Committee of the SCNPC, illustrated the necessity of having the PIPL at the 22nd meeting of the Standing Committee of the 13th NPC. See 'Explanation on the Personal Information Protection Law of the People's Republic of China (Draft)' (13 October 2020) <http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml> accessed 8 February 2022.

[72]PIPL (n 11), Art. 34.

[73]Ibid, Art. 35.

[74]Ibid, Arts. 4(1) and 28.

Table 8. Changes in China's personal information protection regime.

	Before the PIPL	After the PIPL
Material Scope	Exclusion of state actors	Inclusion of state actors
Definitions	Define personal information	Define and distinct personal information and sensitive personal information
Consent	Generally mention	Specify consent requirements and exceptions
Sharing	Generally mention	Outline the obligations of data processors in three scenarios of data sharing
Localization	Generally mention	Outline the requirements for cross-border provision of personal information
Data subjects' rights	Right to rectification (with condition)	Right to information
	Right to erasure (with condition)	Right to access Right to rectification Right to erasure Right to object to processing Right to withdraw consent
Protection	Generally mention	Specify duties of personal information handlers, such as Personal information protection impact assessment
Regulatory authorities	Various government authorities (i.e. CAC, MIIT, SAMR, CBIRC, NHFPC, NMPA, PBOC) have claimed jurisdiction over personal information matters	CAC will be responsible for the overall planning and coordination of the management and supervision of personal information protection Other government authorities manage and supervise personal information protection within their jurisdiction

rules for processing personal information, and requires processing sensitive personal information to meet specific requirements.[75] The PIPL specifies the circumstances in which personal information can be processed, and adopts consent requirements for collecting and processing personal information.[76] It also specifies personal information handlers' notification obligations, including the items, forms, and notification standards.[77] Thirdly, the PIPL also provides individuals with a number of rights regarding processing their personal information, including the right to information, right to access, right to rectification, right to erasure, right to withdraw consent, and right to object to the processing of personal information.[78] It adds personal information protection impact assessment into the list of personal information handlers' duties.[79] Furthermore, the PIPL also sets forth rules regarding data localization and cross-board data transfer.[80] Many of the abovementioned provisions are related to personal information contracting practices. Appendix 3 provides a detailed comparison of the PIPL and GDPR in relation to contracting for personal information.

Another noticeable change brought by the PIPL is that it establishes a well-defined distribution of supervisory power among government authorities. As shown in Table 8, various government authorities have claimed jurisdiction over data-related issues and designed sector-based regulations. These regulators include those supervising industries, such as telecommunications and internet services, banking and finance, healthcare and

[75]Ibid, ch 2, s 2.
[76]Ibid, Arts. 13 and 14.
[77]Ibid, Art. 17.
[78]Ibid, ch 4.
[79]Ibid, Art. 55.
[80]Ibid, ch 3.

e-commerce. The PIPL designates the Cyberspace Administration of China (CAC) as the responsible authority for personal information protection, supported by other state departments.[81]

B. Practical implications and concerns

Views about the impact of the PIPL vary. Some believe that China's PIPL is 'sufficiently in the mainstream of GDPR-influenced laws', which enhances personal information and cybersecurity protection.[82] In contrast, others are more sceptical of the PIPL, worried it will give the Chinese government more powers to monitor data-related companies and reshape Chinese technology giants' business models.[83] While holding different views about the PIPL, scholars and commentators admit that the new law's actual impact awaits its operation in practice.

This study takes a different approach, addressing the impact of the PIPL in response to the three issues identified above related to online contracting for personal information. Firstly, implementing the PIPL will improve the accessibility and readability of personal information protection clauses. The PIPL affirms individuals' rights to be informed about collecting and processing personal information.[84] Individuals also have the right to request data handlers to explain the rules regarding their personal information handling.[85] The PIPL also sets forth obligations for data handlers to notify individuals of the following items using clear and precise language: (1) the data handler's identity and contact information; (2) the categories of personal information being processed, the purpose of processing personal information and the retention period; and (3) methods and procedures for individuals to exercise their rights towards personal information.[86] Similar rules apply to cases where data handlers share or transfer personal information to third parties.[87]

To meet the statutory notification requirements, data handlers need to clarify the purposes and methods of collecting, processing and sharing personal information and the corresponding rights of data subjects. They can do so by adding more data protection clauses to the terms of service or organizing them in separate privacy policies. Thus, it is reasonable to believe that data protection clauses will be made more available to individuals as a result of this law.

Secondly, implementing the PIPL will help promote the standardization of data protection clauses. The survey results in this article indicate that, in practice, because of the lack of a unified data protection law, data handlers, even those in the same industry, adopt different approaches to the definition of personal information, individuals' rights to

[81]Ibid, ch 6.
[82]Graham Greenleaf, 'China's Completed Personal Information Protection: Rights Plus Cyber-security' (2021) 172 *Privacy Laws & Business International Report* 20 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3989775> accessed 8 February 2022.
[83]Arjun Kharpal, 'In a Quest to Rein in Its Tech Giants, China Turns to Data Protection' *CNBC* (11 April 2021) <https://www.cnbc.com/2021/04/12/china-data-protection-laws-aim-to-help-rein-in-countrys-tech-giants.html> accessed 20 April 2021; RogierCreemers, 'China's Emerging Data Protection Framework' (16 November 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3964684> accessed 8 February 2022.
[84]PIPL (n 11), Art. 44.
[85]Ibid, Art. 48.
[86]Ibid, Art. 17.
[87]Ibid, Arts. 22 and 23.

personal information, rules for processing personal information, waivers of liability and dispute resolution. The PIPL has made more explicit rules in these areas. For example, it defines personal information and sensitive personal information and stipulates specific rules for the processing of sensitive personal information.[88] It provides individuals with the right to be informed, to access, correct, and erase personal data and to object to or restrict processing.[89] It also sets forth detailed obligations for data handlers in relation to the collection, processing and securing of personal information.[90] With unified and detailed rules on personal information protection, one may reasonably expect data protection clauses to become more standardized.[91] Consumers have the opportunity to compare the standard-form data protection clauses and shop for better terms.

However, the issue of one-sided standard form contracts may be difficult to address. Although the PIPL has made important breakthroughs in China's data protection legal regime, providing principles and rules similar to the European Union's General Data Protection Regulation (GDPR),[92] it is still perceived as being less comprehensive than the GDPR.[93] Some principles and rules need to be elaborated on further, perhaps through implementation measures and guidelines. Even when comprehensive rules exist, their ability to facilitate the drafting of fairer data protection clauses could be compromised because of the features of online agreements and consumers' online browsing behaviours.[94] Recent studies show that, while firms have updated their terms of services and privacy policies to incorporate the GDPR rules, they have different contracting practices for personal data.[95] 'These differences were most pronounced in terms covering controller and processor designations, purposes and legal bases for processing, data sharing for the purpose of marketing, and data transfer mechanisms'.[96] Thus, even though China's new data protection regime looks promising, its effectiveness will ultimately depend on how it is enforced in practice and how consumers respond to the firms' changes in contracting for personal data.

VI. CONCLUSION

In China, the digital economy has been viewed as an essential component of the national economy, and a clear strategy has been formulated to ensure its development. In the

[88]Ibid, ch 2, s 2.
[89]Ibid, ch 4.
[90]Ibid, ch 5.
[91]For discussions about the broad application of standard-form contracts in the electronic age and the corresponding regulatory development, see, e.g. Robert A Hillman and Jeffrey J Rachlinski, 'Standard-Form Contracting in the Electronic Age' (2002) 77 *New York University Law Review* 429. For empirical analysis of standard-form privacy policies, see, e.g. Davis and Marotta-Wurgler (n 17); FlorenciaMarotta-Wurgler, 'Self-Regulation and Competition in Privacy Policies' (2016) 45 *Journal of Legal Studies* 13.
[92]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter 'General Data Protection Regulation'), OJ 2016 L 119/1.
[93]See Geller (n 66) 1202.
[94]For discussions about the features of online agreements, see, generally, Nancy S Kim, *Wrap Contracts: Foundations and Ramifications* (CUP, 2014); for discussions about internet contractors' browsing behavior, see eg, FlorenciaMarotta-Wurgler, 'Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's 'Principles of the Law of Software Contracts'' (2011) 78 *University of Chicago Law Review* 165.
[95]Davis and Marotta-Wurgler (n 17).
[96]Felicity Turton and others, 'Privacy in the Clouds, Revisited: An Analysis of the Privacy Policies of 40 Cloud Computing Services' Queen Mary Law Research Paper No. 354/2021 (9 April 2021) 66<https://ssrn.com/abstract=3823424>accessed 8 February 2022.

development of a digital economy, the use of data is paramount. In this regard, China's legal framework regarding data protection is inevitably the focus of international attention. China's legislation on data protection is controversial among scholars and practitioners. However, their arguments have not yet been empirically examined. This study contributes some hard facts to the ongoing discussion on the influence of China's data protection legislation.

The study first examines China's legal framework regarding the protection of personal information before the PIPL took effect. It argues that the fragmented legal framework could not adequately protect users' personal information. The study then uses a case study of the P2P sector to demonstrate the inadequate protection reflected in online contracting for personal information. It identifies three key issues in this area after performing a systematic content analysis of terms of service and privacy policies from 202 P2Ps. Firstly, the low level of accessibility and readability of privacy policies raises questions about whether users have been fully informed about the collection, use, and protection of their personal information when registering for network services. Secondly, marked differences are observed between terms of service and privacy policies regarding the types of personal information collected, their processing, sharing, protection rights of data subjects and dispute resolution options, which render them virtually incomparable. Thirdly, terms of service and privacy policies are generally designed to favour online service providers that collect large amounts of personal information and share it with affiliated companies, third-party service providers and relevant governmental authorities.

The study continues to discuss whether the three issues can be addressed by the newly issued, more comprehensive PIPL. It argues that, even though the new law looks promising in general and may address some of the issues found, such as the low level of accessibility and readability to privacy policies and the variations among contractual terms, its effectiveness ultimately depends on its implementation and the digital industry's response. Thus, this study calls for further empirical research on online contracting for personal information in China.

Acknowledgements

I am grateful for the support of the Faculty of Law, Macau University of Science and Technology. My sincere thanks to Dora Neo, Sandra Booysen, Jiwei Qian, Yin Hu, Benjamin Wong and other participants at the working paper presentation organized by the Centre for Banking & Finance Law of NUS Law on 6 July 2021 for their valuable comments and suggestions.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Qin Zhou http://orcid.org/0000-0002-7192-3887

Appendices

Appendix 1. List of Legal Instruments Regarding Personal Information Protection in China

Categories	Name of Legal Instruments	Issuers	Date effective	Key Points
Law (promulgated or released by the NPC or SCNPC)	Personal Information Protection Law of the PRC	SCNPC	1 Nov. 2021	China's first specialized law for personal information and data protection.
	Data Security Law of the PRC	SCNPC	1 Sep. 2021	Puts forward detailed rules for data security.
	Civil Code of the PRC	NPC	1 Jan. 2021	Incorporates an individual chapter that stipulates definition (Art. 1034) principles (Srt. 111 and 1035), rights and responsibilities (Art. 1037–1039 and 1226) regarding personal information and exemptions (Art. 999 and 1036).
	E-Commerce Law of the PRC	SCNPC	1 Jan. 2019	Puts forward principle of e-commerce business to collect, use and protect users' personal information.
	Cybersecurity Law of the PRC	SCNPC	1 June 2017	Defines personal information (Art. 76(5)), and puts forward the obligation of network operators to protect users' personal information (Art. 41, 42 and 64), and the rights of users (Art. 43).
Departmental rules (promulgated or released by the ministries, commissions and other departments with administrative responsibilities directly under the State Council, the PBOC	Implementing Measures of the People's Bank of China for Protecting the Rights and Interests of Financial Consumers	PBOC	1 Nov. 2020	Stipulates definition (Art. 28), principles (Art. 8), rights and responsibilities regarding consumer financial information (Art. 29–34, 41 and 60).
	Measures for the Ascertainment of Illegal Collection and Use of Personal Information	CAC, MIIT, MPS and SMAR	28 Nov. 2019	Provides a reference for relevant regulators to determine the Apps' illegal collection and use of personal information as well as for the App operators to conduct self-examination.
	Provisions on Online Protection of Children's Personal Information	CAC	1 Oct. 2019	Puts forward rules specifically formulated to protect minors' personal information.
	Regulations on Cybersecurity Classification Protection (Draft for Comments)	MPS	27 June 2018	Puts forward the obligation of network operators to establish and implement important data and personal information security protection systems (Art. 31, 65 and 66).
	Provisions on Protecting the Personal Information of Telecommunications and Internet Users	MIIT	1 Sept. 2013	Provides rules for improving the personal information protection in the telecommunications and Internet industries.

(*Continued*)

Appendices Continued.

Categories	Name of Legal Instruments	Issuers	Date effective	Key Points
Notice, Guidelines, Guiding Opinions, Specification and Judicial Interpretation (issued by government authorities, the SPC or SPP)	Information Security Technology – Personal Information Security Specification	SAMR and SAC	1 Oct. 2020	Addresses the issues relevant to the personal information processing, such as collection, storages, use, sharing, transfer, disclosure.
	Personal Financial Information Protection Technical Specification	PBOC	13 Feb. 2020	Provides standards to enhance personal financial information protection.
	Guidelines on Internet Personal Information Security Protection	MPS	19 April 2019	Puts forward more specific implementation of the cybersecurity law regarding personal information security.
	Interpretation on Several Issues on the Application of Law to the Adjudication of Criminal Cases involving the Infrigement of Citizens' Personal Information	SPC and SPP	1 June 2017	Provides clear standards on adjudicating criminal cases involving the infringement of citizen's perfonal information.
	Emergency Response Plan for Cybersecurity Incidents	CCAC	10 Jan. 2017	Puts forward rules and procedures regarding cybersecurity incidents.

*Appendix 2. Categories of personal information**

Categories (level 1)	Categories (level 2)	Items
Sensitive personal information	Background information	name, age (date of birth), gender, ethnicity, religion, nationality, sexual orientation, marital status, family relationship
	Personal identification information	ID card, passport, exit-entry permit, driving license, work permit, residence permit, military ID card
	Biometric information	fingerprint, voiceprint, palm print, pinna, facial recognition, keystroke dynamics, behavioural profiling
	Assets status information	salary, source of income, annual household income, financial assets (wealth management products, bonds, stocks, funds, insurance), fixed assets, real estate, vehicle, virtual currency, virtual assets User
None-sensitive personal information	Third-party linked account	QQ, WeChat, Weibo, Taobao account, Alipay account
	Educational information	diploma, transcript, educational institution
	Employment information	occupation, position, employer, industry type, office address, office phone number
	Personal contact details	mobile phone number, telephone number, email, correspondence address, home address, call details, short message service, multimedia messaging service
	Online behavioural information	website domain, page path, page URL, access record (content, date, time), screen resolution, behaviour logs, browser type, browser history logs, software usage records
	Hardware device information	device ID, name, model, serial number, operating system, SIM card number, battery status, media access control address, identifier for advertisers, international mobile equipment identity number, unique device identifier, international mobile subscriber identity
	Software/application information	application information, application list, software information, software list
	Internet device information	Network information API, Wi-Fi, Bluetooth, hotspot, network operator
	Contact person information	contact person name, phone number, address book, friend list, email address list
	Location information	track locations, latitude and longitude, coordinates, geographic locations, actual locations
	Internet identification information	account, user name, IP address, personal digital certificate
	Personal banking information	bank account, debit card, credit card, deposit records, payment records, transaction records, cash flow, bank account statement, credit card statement
	Investment experience information	risk appetite, risk tolerance, portfolio, investment objectives, investment years
	Personal credit information	sesame credit, criminal records, litigation records, overdue loan records, credit score, PBOC personal credit report
	Personal social welfare information	national social security fund account number, mandatory provident fund account number
	Other personal information	photo album, calendar

* Author referred to the classification standards for sensitive and non-sensitive information used in Information Security Technology – Personal Information Security Specification (GB/T 35273–2020.

Appendix 3. A comparision of the PIPL and GDPR in relation to contracting for personal information

	PIPL	GDPR
Format		
Method of presenting	Personal information handlers shall explicitly notify individuals truthfully, accurately, and fully of the prescribed items (Art. 17)	The data controller shall present the request for consent in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form (Art. 7(2))
Language	Personal information handlers must use clear and easily understood language to present items (Art. 17)	The controller shall use clear and plain language (Art. 12(1))
Content		
Data collection and use	Personal information includes all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons. It does not include information that has been anonymized (Art. 4);	Personal data means any information relating to an identified or identifiable natural person such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Art. 4);
	Personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons 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 personal information of minors under the age of 14 (Art. 28).	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Art. 9(1)).
Data sharing	Where personal information handlers entrust the handling of personal information, they shall conclude an agreement with the entrusted person on the purpose for entrusted handling, the time limit, the handling method, categories of personal information, protection measures, as well as the rights and duties of both sides, etc., and conduct supervision of the personal information handling activities of the entrusted person (Art 21).	Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (e) the recipients or categories of recipients of the personal data, if any (Art. 13(e)).
Rights of data subjects	Individuals have the right to consult and copy their personal information from personal information handlers, except in circumstances provided in Article 18, Paragraph 1, or Article 35 of this Law (Art. 45);	The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information (Art. 15);
	Where individuals discover their personal information is incorrect or incomplete, they have the right to request personal information handlers to correct or complete their personal information (Art. 46);	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement (Art. 16);
	Individuals have the right to know and the right to decide relating to their personal information, and have the right to limit or refuse the handling of their personal information by others, unless laws or administrative regulations stipulate otherwise (Art. 44);	The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions (Art. 21);
	Personal information handlers shall proactively delete personal information where one of the following circumstances occurs; if the personal	The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and

(*Continued*)

Continued.

	PIPL	GDPR
	information handler has not deleted it, individuals have the right to request deletion (Art. 47);	the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies (Art. 17);
	Where personal information is handled based on individual consent, individuals have the right to rescind their consent. Personal information handlers shall provide a convenient way to withdraw consent (Art. 15).	The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing (Art. 17(1)(b)).
Dispute resolution	Personal information handlers shall establish convenient mechanisms to accept and handle applications from individuals to exercise their rights. Where they reject individuals' requests to exercise their rights, they shall explain the reason (Art. 50).	Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation (Art. 77);
	Where personal information handlers reject individuals' requests to exercise their rights, individuals may file a lawsuit with a People's Court according to the law (Art. 50).	Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them (Art. 78(1)).