# ABUSES OF DOMINANCE INVOLVING PERSONAL INFORMATION IN CHINA

BY SÉBASTIEN J. EVRARD, FELICIA CHEN & HAYLEY SMITH[1]



1 Sébastien Evrard is an antitrust partner based in the Hong Kong office of Gibson Dunn & Crutcher. Felicia Chen & Hayley Smith are associates in the same office. The authors wish to thank Professor Angela Zhang for her thoughtful comments. The opinions expressed in this publication are those of the authors. They do not purport to reflect the opinions or views of the firm or its clients.

# CPI ANTITRUST CHRONICLE MARCH 2022 - China Edition


**Identifying an Appropriate Legal Framework for Minimum Resale Price Maintenance: Experiences from the EU and the U.S.**
*By Zhu Li*

**Abuses of Dominance Involving Personal Information in China**
*By Sébastien J. Evrard, Felicia Chen & Hayley Smith*

**Entering the Storm: An Overview of Recent Anti-monopoly Investigations in China**
*By MA Chen & GUO Jiahao*

**Antitrust Regulation in the Automotive Sector: Managing Risks in the BEV Era**
*By Wenting Ge & Hazel Yin*

**China's Practice in Finding Market Dominance of Online Platforms**
*By WU Peng, LONG Rui & DONG Ke*

**New Developments in China Merger Review**
*By Yizhe Zhang & Peter Wang*

**The Past and Future of SEP Antitrust in China**
*By Alexandra (Pu) Yang & Fan Guo*

**Development of Adjudicating Global FRAND Rate in China: A review of *OPPO v. Sharp***
*By Guanbin XIE, Shan JIAO & Qing YING*

**Competition Policy and Regulation in China's Digital Economy**
*By Huang Yong*


Visit www.competitionpolicyinternational.com for access to these articles and more!





## Abuses of Dominance Involving Personal Information in China

*By Sébastien J. Evrard, Felicia Chen & Hayley Smith*


China's recently adopted Personal Information Protection Law ("PIPL") is a new weapon in its arsenal to tame big tech companies. As the first comprehensive legislation to protect personal information within China, the PIPL was adopted amidst a broad regulatory assault on Chinese big tech companies by multiple enforcement agencies, including the State Administration for Market Regulation ("SAMR"), which is responsible for enforcing the PRC Anti-Monopoly Law ("AML"). The PIPL's adoption will have a profound impact on the enforcement of the AML and, in this paper, we explore the interplay between the AML and the PIPL, in particular as it relates to abuses of dominance. We examine the jurisdictional challenges that may arise when anticompetitive conduct involves breaches of the PIPL. In addition, we analyze how the strict criteria for handling personal information under the PIPL may impact SAMR's ability to address the potential anticompetitive effects of abuses of dominance. As an increasing number of courts and administrative agencies outside of China are dealing with issues at the intersection of competition and data privacy laws, with the adoption of the PIPL, issues involving both the AML and the PIPL will soon also come to the forefront in China.

# I. INTRODUCTION

China has (finally) adopted a comprehensive data protection law, the Personal Information Protection Law of the People's Republic of China ("PIPL").[2]

The PIPL was adopted amidst a broad regulatory assault on Chinese big tech companies by multiple enforcement agencies, including the State Administration for Market Regulation ("SAMR"), which is responsible for enforcing the PRC Anti-Monopoly Law ("AML").[3] The PIPL is undoubtedly part of the arsenal of measures that the PRC government has adopted to tame big tech companies.

The adoption of the PIPL also comes at a time when multiple enforcement agencies around the world have devoted considerable resources to better understand the interplay between competition laws and data privacy[4] and, in some cases, aggressively enforce their competition laws in relation to breaches of privacy regulations.

The purpose of this contribution is to explore the interplay between the AML and the PIPL, in particular as it relates to abuses of dominance. Our conclusion is that there is a significant risk that both laws will be enforced against the same conduct such that companies would be punished twice. In this respect, it seems that the PIPL is a more suitable tool to police conduct involving personal information, even if in breach of the AML, because its enforcement agencies do not have to demonstrate the existence of a dominant position or of anticompetitive effects.

In addition, the strict criteria for handling personal information under the PIPL may impact enforcement of the AML. First, it will be more difficult for new entrants to request access to the incumbent's datasets of personal information. Indeed, the obligation to obtain consent from users should be a valid reason for any data owner in a dominant position to reject such request. Second, and for the same reason, the PIPL could also limit SAMR's ability to impose a remedy, such as a transfer of data including personal information, to address the potential anticompetitive effects of abuses of dominance (or of a merger). With the PRC State Council calling for stronger antitrust and data privacy legislation and enforcement, issues at the intersection of the PIPL and the AML will increasingly be at the forefront in China.

# II. LEGISLATIVE FRAMEWORK

### *A. The PIPL*

The PIPL came into effect on November 1, 2021. The PIPL is China's first comprehensive legislation to protect personal information rights of natural persons within China. The PIPL is the primary piece of legislation that protects personal data in China and supplements a patchwork of data privacy-related legislations, including the Cybersecurity Law[5] and the Data Security Law,[6] to create a fulsome regulatory framework regarding cybersecurity and data privacy protection in China.[7]

2 For an English translation of the PIPL, see https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021.

3 See, e.g. SAMR's USD 2.8 billion fine on Alibaba: https://www.samr.gov.cn/xw/zj/202104/t20210410_327702.html.

4 See e.g. Competition Policy for the Digital Era (Directorate-General for Competition, European Commission, 2019); Report of the Study Group on Data and Competition Policy in Japan (Japan Fair Trade Commission, 2019); Digital Platforms Enquiry – Final Report (Australia Competition and Consumer Commission, 2019); Competition and Data Protection in Digital Markets: A Joint Statement between the CMA and the ICO (Competition and Markets Authority and the Information Commissioners Office, 2021); FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets (Federal Trade Commission, 2019).

5 For an English translation of the Cybersecurity Law, see https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

6 For an English translation of the Data Security Law, see https://digichina.stanford.edu/news/translation-data-security-law-peoples-republic-china.

7 The Cyberspace Administration of China ("CAC") is considering draft management rules on cyber-data security for online platform operators to implement the data security articles currently set forth in the Cybersecurity Law, Data Security Law and PIPL. See the full text of the draft management rules in Chinese at http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm. Furthermore, on January 6, 2022, CAC also made public the draft Provisions on the Administration of Mobile Internet Application Information Services. The new draft provisions revise the currently in-effect Regulation on the Administration of Mobile Internet Application Information Services to impose additional legal obligations on app distribution platforms and clarify existing legal obligations. See the full text of the draft provisions at http://www.gov.cn/xinwen/2022-01/05/content_5666589.htm.

The PIPL creates new rights of actions for individuals whose personal information rights are violated, as well as requirements and penalties for personal information handlers ("PIH") that violate this law. The PIPL shares many similarities with the European Union's General Data Protection Regulation (the "GDPR"),[8] including, amongst others, the extraterritorial effect, the creation of personal information rights, and penalties for PIH in case of breaches.[9] The PIPL is broad in scope and its interpretation will depend on guidance documents, new regulations and standards, and enforcement actions by authorities, which are only beginning to be published at this stage.[10]

The purpose of the PIPL is to protect personal information rights, standardize activities around personal information processing[11] and encourage the reasonable use of personal information.[12] The PIPL applies to PIHs[13] who process personal information of natural persons within China.[14]

The scope of personal information processing is limited to that which has a "clear and reasonable purpose" and is "directly related to the processing purpose," in order to minimize the impact on individuals' rights and interests.[15] The PIPL adopts principles of transparency towards personal information processing, which includes disclosing to individuals the rules for processing personal information and clearly indicating the purpose, method, and scope of such processing.

There is a limited list of legal grounds for PIHs to process personal information. This includes obtaining individuals' consent,[16] which must be given with full knowledge and in a voluntary and explicit statement.[17] If there is a change to the purpose or method of such processing or to the categories of processed personal information, individual consent will need to be obtained again.[18] Individual consent may also be re-scinded and PIHs must provide a convenient way to withdraw such consent.[19] If an individual does not provide consent or rescinds his consent, PIHs may not refuse to provide their products or services to that individual except where processing personal information is necessary to provide such product or service.

There are limited circumstances in which PIHs may process personal information without individual consent, including where necessary to fulfil a contract in which the individual is an interested party or to fulfil statutory duties.[20] In the event that personal information needs to be transferred due to a merger, the PIH must notify individuals regarding the name and contact method of the receiving party, which will have to continue to fulfil the PIH's obligations.[21] If the receiving party changes the original processing purpose or method, it will need to obtain individual consent again,[22] which may be withdrawn.[23]

---

8 A copy of the official legal text of the GDPR is available at https://gdpr-info.eu/.

9 There are also many differences between the GDPR and the PIPL. See https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/.

10 Administrative agencies have started to issue notices and guidance documents in response to PIPL. For example, the Shanghai Municipal Administration for Market Regulation has issued a set of guidelines to assist online platforms' compliance with various laws, including PIPL, when using algorithms to conduct sales activities. See the full text of the guidelines in Chinese at https://www.shanghai.gov.cn/gwk/search/content/2c9bf2f67d043165017d30e80ce54da0.

11 The term used in the Chinese text for "handling" is "处理," which we will translate interchangeably in "processing" and "handling."

12 See Article 1 of the PIPL.

13 The term used in the PIPL is "个人信息处理者," which can be translated into "personal information handlers." We will use the term "PIH" throughout this article.

14 See Article 3 of the PIPL. Personal information refers to "all kinds of information, recorded by electronic or other means, related to identifiable or identifiable natural persons, not including information after anonymization handling."

15 See Article 6 of the PIPL.

16 Article 13 of the PIPL. One of the differences with the GDPR is that under the PIPL "legitimate interest" is not a legal ground for processing personal data.

17 See Article 14 of the PIPL.

18 *Id.*

19 See Article 7 of the GDPR and Article 15 of the PIPL.

20 See Article 13 of the PIPL. Importantly, "legitimate interest" is not a legal ground for processing personal information, an important difference with the GDPR.

21 See Article 22 of the PIPL.

22 See Articles 14 and 22 of the PIPL.

23 See Article 15 of the PIPL.

The PIPL gives agencies at different levels enforcement power over its regulations. The State cybersecurity and informationization department is responsible for planning and coordinating personal information protection work, as well as carrying out related supervision and management.[24] Relevant departments under the State Council are responsible for enforcing the PIPL to the extent enforcement falls within their respective scope of duties, and relevant departments at the county-level and higher people's governments are responsible for enforcing the PIPL according to relevant State provisions (together with the State cybersecurity and informationization department, the "PIPL Enforcement Agencies").

The PIPL Enforcement Agencies can impose sanctions for breaches of the PIPL. They can order PIHs to correct their conduct, confiscate their unlawful income and order the suspension of any application programs unlawfully handling personal information.[25] In the event the PIH refuses such correction, the PIPL Enforcement Agencies can impose a fine of up to RMB 1 million on the PIH and a fine between RMB 10,000 and RMB 100,000 on directly responsible personnel.[26] Additionally, for grave[27] violations, the penalties are more severe. The PIPL Enforcement Agencies can fine the PIH up to RMB 50 million (or 5 percent of annual revenue),[28] suspend the PIH's business activities as well as cancel the PIH's administrative or business licenses.[29] The PIPL Enforcement Agencies can also fine directly responsible personnel between RMB 100,000 and 1 million and they may ban such personnel from holding positions of director, supervisor, high-level manager or personal information protection officer for an unspecified period of time.[30]

Finally, PIHs may be liable for any harm resulting from the breach of the PIPL if they fail to prove they are not at fault.[31] Compensation is determined based on either the resulting loss to the individual or the benefits that accrue to the PIH.[32] If such calculation methods are hard to determine, compensation is to be determined according to "practical conditions."[33] The PIPL also allows for certain groups, which are the People's Procuratorates, statutorily designated consumer organizations and organizations designated by the state's cybersecurity and informatization department, to file a lawsuit with a People's Court when PIHs have committed infringements of the rights of many individuals.[34]

### *B. The AML*

The AML came into force in 2008.[35] It includes a prohibition on anticompetitive agreements between competitors, including price-fixing, output restrictions, market allocation and boycotts.[36] It also prohibits vertical agreements that restrict or eliminate competition, including resale price maintenance.[37] Certain agreements may benefit from an exemption of the prohibition on anticompetitive agreements where they, essentially, have pro-competitive consumer benefits.[38]

24 See Article 60 of the PIPL.

25 See Article 66 of the PIPL.

26 *Id.*

27 The PIPL does not define what qualifies as "grave."

28 The PIPL does not provide the method for determining annual revenue.

29 See Article 66 of the PIPL.

30 *Id.*

31 *Id.*

32 See Article 69 of the PIPL.

33 *Id.*

34 See Article 70 of the PIPL.

35 On the AML generally, see S. Harris, P. Wang, Y. Zhang, M. Cohen & S. Evrard, Anti-Monopoly Law and Practice in China, Oxford University Press, 2011.

36 See Article 13 of the AML.

37 See Article 14 of the AML.

38 See Article 15 of the AML.

The AML also prohibits abuses of a dominant position.[39] This includes selling products at unfairly high prices, selling below costs, refusals to deal, tying and discrimination.[40] The AML includes a presumption of dominance where a single undertaking's market share exceeds 50 percent.[41]

Finally, the AML includes a pre-closing merger control system. Mergers exceeding certain revenue thresholds must be notified to SAMR and cannot be closed before clearance. SAMR will review whether the transaction results or may result in the elimination or restriction of competition. In that case, SAMR has the power to prohibit a transaction. Parties to a transaction may offer remedies to address any concerns, in which case SAMR may conditionally approve the transaction.

In terms of sanctions, SAMR may impose a fine between 1 and 10 percent of a company's turnover in case of a breach of the prohibition on anticompetitive agreements or abuses of dominance. The fine for a breach of the obligation to notify transactions is limited to RMB 500,000, but SAMR can unwind a deal if it comes to the conclusion that such deal is anticompetitive.[42] SAMR can also confiscate illegal gains.

Over the years, SAMR and its predecessors have issued a host of guidelines. For the purpose of this contribution, we refer in particular to the Antitrust Guidelines in the Field of Platform Economy ("Platform Guidelines")[43] and the Interim Provisions on Prohibiting Acts of Abuse of Dominant Market Position ("Abuse of Dominance Guidelines").[44]

## III. JURISDICTIONAL ISSUES

The PIPL's adoption will have an impact on the enforcement of the AML. Indeed, we consider that some anticompetitive conduct will involve breaches of the PIPL such that both enforcement agencies may have jurisdiction (and impose sanctions).nWe also consider whether the PIPL has curtailed SAMR's ability to enforce the AML, or at least SAMR's ability to impose some remedies involving the transfer of personal information.

### *A. Dual Enforcement of Anticompetitive Conduct Involving Breaches of the PIPL*

SAMR and the PIPL Enforcement Agencies will both have jurisdiction over anticompetitive conduct involving breaches of the PIPL. It is unclear whether and how they will coordinate their enforcement actions.[45] This creates a risk that a company could be fined twice for the same conduct.[46]

In China, there is a significant risk of dual enforcement, which is that both SAMR and the PIPL Enforcement Agencies would investigate (and potentially impose a fine for) conduct that is in breach of both the PIPL and the AML. While the Administrative Penalty Law ("APL")[47] includes a provision against double jeopardy, it is unlikely to provide meaningful protection against dual enforcement. Article 29 of the APL provides that *"[t]he administrative fine shall not be imposed more than once for the same violation of law by a party. Where an illegal act violates several legal provisions, with each of them imposing a fine on such act, the provision that imposes the heaviest fine shall apply."* According to a literal reading of this provision, double jeopardy only applies in case of two violations of the same law. This would mean that double jeopardy does not apply when the same act violates two different laws, such as the PIPL and the AML.

39 See Article 17 of the AML.

40 See Article 17 of the AML.

41 See Article 19 of the AML. The presumption of dominance also applies where two undertakings have a combined market share in excess of 66 percent, or three undertakings have a combined market share in excess of 75 percent. These presumptions are based on combined market shares do not apply to an undertaking that has a market share below 10 percent.

42 See Article 48 of the AML.

43 See the full text of the Platform Guidelines in Chinese at https://gkml.samr.gov.cn/nsjg/fldj/202102/t20210207_325967.html.

44 See the full text of the Abuse of Dominance Guidelines in Chinese at https://gkml.samr.gov.cn/nsjg/fgs/201907/t20190701_303057.html.

45 We are already starting to see challenges to PIPL enforcement between regulators at different levels. On December 9, 2021, the Shanghai market regulator and Shanghai Municipal Economic and Informatization Commission issued guidelines to boost digital advertising in the city. The guidelines' approach to data security were more lenient than the PIPL's and which marks a divergence between the interests of central and local regulators.

46 This issue has arisen is other jurisdictions. See, e.g. European Court of Justice, case C -252/21, *Facebook Inc., and Others v. Bundeskartellamt*, in which one of the questions submitted to the Court relates to the German competition authority's jurisdiction over an alleged abuse of dominance involving personal data in view of the ongoing data privacy investigation in another EU Member State. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CN0252.

47 For an English translation, see http://www.npc.gov.cn/englishnpc/c23934/202105/f18b60e2b2ed4198ab12fa3ac999fc5a.shtml.

Enforcing both laws for the same conduct would be a considerable waste of the government's resources and could put a significant burden on PIHs. It would therefore be recommended that the respective jurisdictions of SAMR and the PIPL Enforcement Agencies be delimited, for example through a memorandum of understanding. In this respect, there are small differences in their enforcement powers such that, depending on the circumstances, one or the other agency may be better placed to investigate and, as the case may be, put an end to the alleged conduct.

Both agencies have wide powers to conduct their investigation and, in particular, both can conduct dawn raids, interview relevant individuals and seize documents.[48] Both can ask the PIH to cease and desist the infringing conduct.[49] While both can impose a fine, it seems that for non-grave breaches, the PIPL Enforcement Agencies can only impose a fine if the PIH refuses to "correct" its conduct.[50] Provincial or higher-level departments fulfilling personal information protection duties are responsible for imposing fines and ordering correction for grave violations.[51]

The amount of the fines that they can impose is also different: while the PIPL distinguishes between non-grave (maximum RMB 1 million) and grave (maximum 50 million or 5 percent of revenues) violations, SAMR can impose fines of up to 10 percent of turnover, regardless of the gravity of the infringement.[52] The PIPL Enforcement Agencies can impose fines (and other sanctions) on individuals while SAMR can only impose fines on undertakings. Finally, both can order the confiscation of the illegal income stemming from the infringement.

Abuses of dominance is the area where there is the highest risk of dual enforcement. It seems that, in many cases involving abuses of dominance where the alleged conduct is also a breach of the PIPL, the PIPL Enforcement Agencies may be better placed to investigate as they do not need to demonstrate the existence of a dominant position or of the conduct's effects on the market. This would, for example, be the case where the allegation is that a PIH in dominant position is engaging in exploitative abuse such as harvesting personal data in breach of the PIPL or making the use of its service contingent upon the processing of personal information beyond what is strictly necessary.

### *B. SAMR's Ability to Request Information from Third Parties*

SAMR routinely sends requests for information to parties under investigation and/or to third parties in order to gather data for the purpose of its investigation into a particular conduct. This power is enshrined in Article 39 of the AML and a refusal to provide the requested information is subject to penalties under Article 52 of the AML.

Responding to these requests for information regularly involves the disclosure of personal information. For example, internal documents may reveal the identity of a company's employees. In order for SAMR to obtain such information and process it lawfully, the PIH must be able to rely on a legal ground to disclose the information to SAMR and, in addition, SAMR must have a legal ground to process the personal information.

PIH are likely to be able to rely on Article 13(2) of the PIPL to disclose personal information to SAMR, this is "where necessary to fulfil statutory duties and responsibilities or statutory obligations." As explained above, PIHs have a legal obligation to respond to SAMR's request for information.

Article 34 of the PIPL may serve as a ground for SAMR to collect and process personal information: *"State organs handling personal information to fulfil their statutory duties and responsibilities shall conduct them according to the powers and procedures provided in laws or administrative regulations; they may not exceed the scope or extent necessary to fulfil their statutory duties and responsibilities."* This provision, however, seems to call for a specific law or administrative regulation to deal with the processing of personal information, which SAMR has not yet published.[53]

---

48 See Article 63 of the PIPL and Article 39 of the AML.

49 The PIPL enables the PIPL Enforcement Agencies to "correct" the breach, which should be substantially the same as the SAMR's ability to order a "cease and desist."

50 In the absence of any definition of a "grave" breach, the PIPL Enforcement Agencies are likely to take an expansive view of that term.

51 See Article 66 of the PIPL.

52 According to Article 49 of the AML, SAMR will take the seriousness of the violation into account when determining the amount of the fine. The highest fines imposed thus far by SAMR for abuses of dominance include a USD 2.8 billion fine against Alibaba and a fine of nearly USD 1 billion against Qualcomm. See SAMR's decision against Alibaba in Chinese at https://www.samr.gov.cn/fldj/tzgg/xzcf/202104/t20210409_327698.html, and the decision against Qualcomm in Chinese at https://www.samr.gov.cn/fldj/tzgg/xzcf/202101/P020210126539901257191.docx.

53 See, in the European Union, the Commission Decision (EU) 2018/1927 of 5 December 2018 laying down internal rules concerning the processing of personal data by the European Commission in the field of competition in relation to the provision of information to data subjects and the restriction of certain rights, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018D1927.

This being said, where the identity of specific individuals is not necessary for the purpose of investigating a particular conduct, it is questionable whether SAMR has the power to request such personal information. Indeed, as explained above, one of the fundamental principles of the PIPL is that "the collection of personal information shall be limited to the smallest scope for realizing the handling purpose, and excessive personal information collection is prohibited."[54] For example, in the case of a cartel investigation, given that SAMR does not have the power to impose fines on individuals, it is questionable whether SAMR has the power to request the identity of employees as opposed to anonymized data.[55] It is likely, though, that SAMR will take an expansive view of its powers and will take a dim view on any undertaking trying to resist the disclosure of employee details. This may, however, put some companies at risk of violating their employees' rights if they disclose personal information without a legal ground.

### *C. AMR's Ability to Order Remedies Involving Personal Information*

In case of a breach of the prohibition on anticompetitive agreements or of abuses of dominant position, SAMR can order the undertaking to "cease and desist" such acts. Parties under investigation can also offer "commitments" to suspend the investigation. As regards merger control, SAMR has the ability to accept commitments (including, for example, a divestiture of assets) to conditionally approve a transaction.

Some of these measures may require a PIH to transfer personal information protected under the PIPL to third parties. For example, in the case of a refusal by a PIH to grant access to personal information protected under the PIPL to a competitor, SAMR may want to order the PIH to grant such access. In the case of a merger requiring a divestiture, the divested assets may include personal information.

SAMR seems to consider that, in the merger context, it has the power to impose a remedy that requires the processing of personal information protected under the PIPL. Article 21 of SAMR's Platform Guidelines states that SAMR may impose "structural conditions such as divestiture of tangible or intangible assets such as intellectual property, technology and data or divestiture of relevant interests" as well as "behavioral conditions such as opening of infrastructures such as networks, data or platforms, licensing key technologies, terminating exclusivity agreements, modifying platform rules or algorithms, committing to compatibility or no reduction of interoperability levels, etc."

However, these guidelines were drafted before the adoption of the PIPL and the strict provisions of the PIPL may curtail SAMR's ability to impose such measures. Indeed, a PIH can only transfer personal data to a third party in a limited set of circumstances listed in Article 13 of the PIPL.

The most relevant legal grounds for transferring data as part of a commitment are Article 13(1) of the PIPL (consent) and Article 13(3) of the PIPL (which authorizes data processing "where necessary to fulfil statutory duties and responsibilities or statutory obligations"), which does not require consent from the individual.[56]

In case the merger parties offer a commitment to SAMR in order to obtain a conditional approval for their transaction, it seems that Article 13(3) of the PIPL would not apply as the transfer of personal information is a voluntary process and not in pursuance of a legal or statutory obligation. Hence, merger parties would have to inform users about the transfer in accordance with Article 22 of the PIPL. Given that individuals can rescind their consent in accordance with Article 15 of the PIPL, there is no guarantee that a commitment, which appears adequate on paper, will in the end have the intended effect.

In the case of an investigation into an alleged refusal to grant access to personal data by a dominant firm, SAMR may want to order the dominant firm to "cease and desist" such conduct, which practically means that access must be granted.

In that case, it is unlikely that the dominant firm will have the individuals' consent to transfer their personal information to the competitor requesting access. The dominant firm will therefore need to obtain such consent in accordance with Article 13 of the PIPL. The other possible ground is Article 13(3) of the PIPL, but it is not obvious that a SAMR decision to cease and desist a specific conduct will constitute a valid "statutory duty and

54 Article 6 of the PIPL.

55 Except if, for example, SAMR wants to interview specific individuals.

56 It seems that Article 22 of the PIPL, which requires PIH to inform users and obtain their consent in case of a transfer to another PIH, would not apply in the case of a statutory obligation to transfer data because Article 13(7) explicitly provides that consent is not required.

responsibility" or a "statutory obligation"[57] to transfer such data.[58] Further guidance would be required, for example by adopting a specific law or regulation specifying that SAMR decisions are to be considered as a statutory duty and responsibility or statutory obligation under Article 13(3) of the PIPL.

## IV. ABUSES OF DOMINANCE INVOLVING PERSONAL INFORMATION

An increasing number of courts and administrative agencies outside of China have had to deal with issues at the intersection of competition and data privacy laws. This is not a surprise given the importance of data in today's economy. With the adoption of the PIPL, in the midst of a crackdown on big tech, issues involving both the AML and the PIPL will soon also come to the forefront in China. In this section, we look at how the AML and the PIPL would be applied to abuses of dominance involving personal information.

### *A. Abusive Processing of Personal Data*

In a series of overseas cases, PIHs have faced allegations that they abused their dominant position by requiring individuals to consent to the processing of personal data in order to use their service.[59] The relevant question is whether a dominant PIH would be in breach of the AML if it were to collect information as a pre-condition for using a particular service.

In China, as explained above, PIHs must obtain users' consent before processing their personal information. Such consent must be based on "full knowledge"[60] and based on the information listed in Article 17 of the PIPL, this is (I) the identity and contact details of the PIH, (ii) the purpose and methods of processing, (iii) the methods and procedure for individuals to exercise their rights, and (iv) other information prescribed by law. In addition, according to Article 6 of the PIPL, "the data shall be collected for clear and reasonable purposes, its collection should be directly related to the processing purpose, and be conducted in a way that minimizes any effect on individual rights." Article 16 also prevents PIHs from refusing to provide a product or service on the basis that the individual does not consent to the handling of their personal information.

Article 17(5) of the AML prohibits undertakings in a dominant position from imposing unreasonable trading conditions. According to Article 18 on the Interim Provisions on Prohibiting Acts of Abuse of a Dominant Market Position, this includes attaching transaction terms that are not relevant to the subject-matter of the transaction. Similarly, Article 16 of the Platform Guidelines provides a non-exclusive list of factors that would be taken into account when determining whether a dominant undertaking is imposing unfair trading conditions. This list includes the "compulsory collection of unnecessary user information […]." Given that the list is not exhaustive, we can assume that forcing individual users to consent to the transfer of their data to third parties (for example, for the purpose of providing targeted advertising) will also be considered as an unfair trading condition.

A PIH in a dominant position that requires users to provide "unnecessary information" (or to consent to a transfer of personal information to a third party) as a condition for using the service could therefore be in breach of both the PIPL and the AML.

In this respect, there is no guidance on the term "unnecessary information." A narrow interpretation would mean that a PIH can only collect information that is strictly necessary to use a service (or deliver a product). In this respect, in July 2021, a local court in Zhejiang province found that Ctrip, the largest online travel agent, was liable for collecting personal data from users that was used to personalize price offering and could result in higher prices for consumers.[61] The court ordered Ctrip to either allow for the plaintiff to use its services without agreeing to the platform's privacy policy and service agreement or stop collecting unnecessary personal information.

57 The term used by the PIPIL is "法定义务" which we have translated as "statutory obligation." The term "statutory obligation" appears to suggest a prerequisite statutory law, order or regulation that would give rise to an obligation to comply. In the present case, a cease-and-desist decision appears to fall short of this requirement.

58 Under Article 6.1(c) of the GDPR, data can be processed where it is "necessary for compliance with a legal obligation to which the controller is subject." It is debatable whether this would be a sufficient ground for allowing access to data under Article 102 TFEU (which prohibits abuses of dominance). Indeed, according to recital 41 of the GDPR "*such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it.*" See V. Kathuria & J. Globonick, Exclusionary conduct in data-driven markets: limitation of data sharing remedies, Max Planck Institute for Innovation and Competition, Research paper No. 19-04, p. 23.

59 For example, in March 2016, Germany's competition authority, the Bundeskartellamt, launched an investigation to assess whether Facebook's data policy infringes Germany's competition law. The case has been referred to the European Court of Justice for a preliminary ruling. Further, in March 2021, the Competition Commission of India ("CCI") ordered a *suo moto* investigation into changes to WhatsApp's privacy policy. Prior to conducting any investigation, the CCI took the *prima facie* position that the changes constituted the imposition of unfair terms. WhatsApp challenged the characterization of its policy update and argued that the CCI should not be able to exercise jurisdiction to initiate an investigation until after parallel judicial challenges before various courts in India are resolved. WhatsApp's jurisdictional challenge to the CCI's decision to open an investigation is currently pending before the Indian courts. See *In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users, Suo Moto Case No. 01 of 202*, available at: https://www.cci.gov.in/sites/default/files/SM01of2021_0.pdf.

60 See Article 14 of the PIPL.

61 See https://www.scmp.com/tech/policy/article/3141264/tripcom-ordered-make-exception-privacy-policy-lawsuit-could-open-door. The legal basis for the rule is unclear.

Any limitation on the amount of information that can be processed could create an issue for services that are funded by advertising and where the service operator collects personal information from its users to offer more targeted advertising and raise revenues. This personal information is arguably not necessary (in a strict sense) to provide the service. A possible workaround would be to provide that the data is in fact the "price" that the user must pay for obtaining the service and that, in the absence of such "payment," the user will be unable to use the service. However, the PIH would still potentially face a competition law claim as Article 17(3) prohibits the imposition of an "unfairly high price."

Enforcement against "unfairly high prices" has been limited in China[62] and it is very much the question how SAMR could determine whether prices are unfairly high. In its Interim Provisions on Prohibiting Acts of Abuse of a Dominant Market Position, SAMR provides that prices are unfairly high when they are (i) significantly higher than prices for comparable products sold by competitors, (ii) significantly higher than the prices applied by the undertaking in other geographic markets, (iii) when the price increases beyond the normal range with stable costs, (iv) when the price raises significantly faster than the increase in costs[63]. In this case, it is unclear whether SAMR could use these factors to assess whether the personal information that the user is required to provide is too extensive.

It seems therefore that guidance is needed on what constitutes "unnecessary information." In addition, it seems that the PIPL Enforcement Agencies will be better placed than SAMR to investigate allegations of processing of unnecessary personal information as they will not have to demonstrate the existence of a dominant position nor of anticompetitive effects.

### *B. Refusals to Deal*[64]

Historically, refusal to deal claims have not been widely successful in China[65] although the Chinese economy is characterized by the presence of monopolies across multiple industries, which should be a fertile ground for such claims.[66]

The PIPL is likely to make such claim more difficult given that the PIH would need to obtain users' consent to transfer their personal information to a third party.[67] Hence refusals to deal involving personal information will only be possible in exceptional cases. This would not be inconsistent with the practice overseas where there have been few cases of refusals to deal involving personal data.

Article 17 of the AML prohibits undertakings with a dominant position from refusing to deal without justified reason. Refusals to deal are not limited to "essential facilities" cases. Indeed, Article 16 of the SAMR Interim Guidelines on the Prohibition of Abuses of Dominance Position clarifies that, in addition to "essential facilities," refusals to deal include interrupting existing transactions, refusing to enter into new transactions, imposing restrictive conditions to make transactions more difficult. As regards "essential facilities," the Guidelines state that to determine whether

62 See the cases listed in Yi Xue & Tian Gu, Competition Enforcement against Unfairly High Prices in China, June 23, 2020, Competition Policy International, available at https://www.competitionpolicyinternational.com/competition-enforcement-against-unfairly-high-prices-in-china/.

63 See Article 14 of the Interim Provisions on Prohibiting Acts of Abuse of a Dominant Market Position.

64 There are two significant cases from the US regarding the intersection of refusals to deal and data privacy. One such case is *HiQ v. LinkedIn*, in which the plaintiff, hiQ Labs ("hiQ"), a data analytics company, scraped information from LinkedIn that users included on public LinkedIn profiles for use in its "people analytics" software. Although LinkedIn initially permitted this access to user data, it later sent hiQ a cease-and-desist letter asserting that hiQ was in violation of LinkedIn's User Agreement and demanding that hiQ stop accessing and copying data from LinkedIn's server. On appeal to the Ninth Circuit, the court found all of hiQ's antitrust claims to be deficient for failure to adequately allege a product market, namely the "people analytics market." The court granted hiQ leave to amend its product market. See *hiQ Labs, Inc. v. LinkedIn Corp*, 938 F.3d 985 (9th Cir. 2019) and *hiQ Labs, Inc. v. LinkedIn Corp*, (Case No. 17-cv-03301-EMC) (Docket No. 137).

The second case is *PeopleBrowsr v. Twitter*. In 2012, PeopleBrowsr brought a lawsuit in US State Court against Twitter for anticompetitive practices by Twitter in seeking to limit access to its data to a select subgroup of companies, excluding PeopleBrowsr. PeopleBrowsr paid Twitter for access to the Twitter "Firehose," through which PeopleBrowsr was able to access every tweet posted on Twitter. PeopleBrowsr sought a temporary restraining order ("TRO") against Twitter, seeking to preserve PeopleBrowsr's access to the Firehose, which Twitter threatened to cut off (para. 2, Application for TRO). The US State Court initially granted PeopleBrowsr's application for a TRO, however the case was eventually settled out-of-court on April 25, 2013. Pursuant to the settlement, PeopleBrowsr was able to continue accessing the Firehose through to the end of 2013, after which it would transition to data access from an authorized Twitter data reseller. *See* https://thenextweb.com/news/peoplebrowsr-vs-twitter (which contains PeopleBrowsr's Application for TRO and Twitter's Opposition to TRO); See also https://casetext.com/case/peoplebrowsr-inc-v-twitter-2?__cf_chl_jschl_tk__=pmd_UWCCWL6.L1__8DlszLB6Uq0VOXAn-wswOdzplfPWasbHM-1631603249-0-qNtZGzNAjujcnBszQs9 (Order Granting Plaintiffs' motion to Remand to State Court).

65 For an example of successful claim in a lower court, see https://www.allenovery.com/en-gb/global/news-and-insights/publications/hitachi-metals-essential-patents-recognised-as-essential-facility-in-china.

66 For more details see S. Evrard & Y. Zhang, Refusal to Deal in China: A Missed Opportunity, in A. Emch & D. Stallibrass (eds) China's Anti-Monopoly Law, the First Five Years, p. 135.

67 The data privacy defense would likely not apply if the complainant asked for access to anonymized data. Indeed, according to Article 4, the PIPL does not apply to data that has been anonymized, this is where it has been processed to ensure it is impossible to identify specific natural persons without the support of additional information.

there is a justification for refusing access to an essential facility, account should be taken of various factors including, essentially, whether it is feasible to duplicate the facility in order to compete effectively on the market.[68]

The Interim Guidelines also set out what could constitute a "justified reason" for refusing to deal, including the fact that conducting the transaction will unduly impair the interests of the operators, as well as "other reasons that can justify the legitimacy of the actions." As regards internet platforms, the Platform Guidelines set out a similar test.

A competitor claiming that a PIH is abusing its dominant position by refusing access to personal data is likely to face an uphill battle.

First, from a competition law point of view, the plaintiff would have to demonstrate that the PIH holds a dominant position. While the AML includes a rebuttable presumption of dominance based on market shares, such market shares may be difficult to calculate in data-related markets. In addition, the Chinese Supreme People's Court ruled in *Qihu v. Tencent* that market shares alone might be an unreliable indicator of market dominance in the internet sector because it is highly dynamic and the boundaries of the relevant market are far less clear than those in traditional sectors.[69]

If the plaintiff claims that the data is an essential facility, it will have to demonstrate that such data is necessary or indispensable to compete. Given that data is non-exclusive and non-rivalrous[70], it is likely that such a claim would fail. Finally, the plaintiff will have to demonstrate that the refusal has an anticompetitive effect.[71]

Second, it seems that the PIPL may provide the PIH with a justified reason for refusing access to personal data. Indeed, a PIH can only transfer personal data to a third party in a limited set of circumstances listed in Article 13 of the PIPL.[72]

The most relevant ground is likely to be 13(1) of the PIPL, which authorizes a PIH to transfer personal data provided it has obtained the user's consent. According to Article 14 of the PIH such consent must be based on "full knowledge." According to Article 23 of the PIPL, before transferring data to a third party, the PIH must notify the individual of the identity of the recipient, the purpose and method for processing the data and obtain consent. Given that a PIH's privacy policy is unlikely to include information about potential transfers of personal data to competitors, the PIH will not have the user's consent to transfer the data. The absence of consent should constitute a justified reason for refusing access to the data.

Another possible ground to justify the transfer of data to a third party seeking access to personal data would be Article 13(3) of the PIPL, which authorizes data processing "where necessary to fulfil statutory duties and responsibilities or statutory obligations." Such ground does

---

68 See Article 13. This test is reminiscent of the test developed by the European Court of Justice in case C 7-97, *Oscar Bronner GmbH v. MediaprintZeitungs- und Zeitschriften-verlag GmbH*, [1998] ECR I-7791. Further on this case, see S. Evrard, Essential Facilities, *Bronner and Beyond*, The Columbia Journal of European Law, 2004, p. 491. More generally, on the application of the essential facilities doctrine to data in Europe, see I. Graef *Rethinking the Essential Facilities Doctrine for the EU Digital Economy*, April 2019, TILEC discussion paper, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3371457. See also Article 7 of the Provisions on the Prohibition of the Abuse of Intellectual Property Rights to Exclude or Restrict Competition; see also Article 16 of the Anti-Monopoly Guidelines of the Anti-Monopoly Committee of the State Council in the Intellectual Property Industry.

69 In two cases of abuse of dominant position involving the use of personal data, the French and Belgian competition authorities concluded that the holder of such data had a dominant position. However, in these cases, the owners had respectively a legal monopoly for the supply of gas and electricity in France and the supply of public lottery services in Belgium. See French Competition Authority, decision 17-D-06 of March 21, 2017 relating to practices in the sector of natural gas, electricity, and energy; Belgian Competition Authority, decision BMA-2015-P/K-28-AUD of September 22, 2015.

70 Non-exclusive, meaning that it may not be possible to prevent others from using the data, and non-rivalrous, meaning that one person's use of data does not reduce another's use of the same data

71 Article 6 of the AML provides that undertakings should not abuse their dominant position to restrict or eliminate competition. In Qihu v. Tencent, the SPC decided that "even if the sued business operator has a dominant market position, determining whether its [act] constitutes an act of abusing a dominant market position requires [the court] to comprehensively assess the negative effects and the potentially positive effects of the act on consumers and competition so as to judge the legality of the act." See 北京奇虎科技有限公司诉腾讯科技（深圳）有限公司、深圳市腾讯计算机系统有限公司滥用市场支配地位纠纷案》*Beijing Qihu Technology Co., Ltd. v. Tencent Technology (Shenzhen) Company Limited and Shenzhen Tencent Computer Systems Company Limited*, A Dispute over Abusing Dominant Market Positions), STANFORD LAW SCHOOL CHINA GUIDING CASES PROJECT, English Guiding Case (EGC78), Apr. 7, 2017 Edition, http://cgc.law.stanford.edu/guiding-cases/guiding-case-78.

72 The data privacy defense would likely not apply if the complainant asked for access to anonymized data. Indeed, according to Article 4, the PIPL does not apply to data that has been anonymized, this is where it has been processed to ensure it is impossible to identify specific natural persons without the support of additional information.

not require consent from the individual.[73] Although the language is vague enough to support the view that access to data would be necessary to comply with the AML, it would seem, that such interpretation would run counter to the objective of the PIPL, which is to grant individuals the right to decide who will process their data and how. In particular, Article 44 of the PIPL explicitly provides that "individuals have the right to know and the right to decide relating to their personal data, and have the right to limit or refuse the processing of their personal data by others, unless laws or administrative regulations provide otherwise"[74]. Therefore, subject to further clarification regarding the scope of Article 13(3) of the PIPL, it would seem unlikely that a request for access to data could be based on the need to comply with statutory obligations.

In any event, it is very much the question whether access to such data would be at all useful for a third party. Indeed, the recipient would have to provide information to individuals under Article 17 of the PIPL[75] and such individuals would have the right to obtain the deletion of their data on the basis of Article 47 of the PIPL. Under these circumstances, it may be easier and less cumbersome for complainants to simply try to obtain personal information directly from individuals.

The courts may have a first opportunity to opine on these issues. In November 2021, the Changsha Intermediate People's Court accepted an antitrust complaint brought by Eefung Software, a network public opinion monitoring company based in Hunan province. Sina Weibo allegedly terminated its cooperation with Eefung Software, which then attempted to reconnect with Sina Weibo to no avail. Eefung Software alleges that its business model was destroyed by such termination. Eefung Software is accusing Sina Weibo of refusing to deal and is seeking the use of Sina Weibo's data under reasonable conditions, as well as compensation for economic loss and reasonable legal costs.[76] This case will likely be a precedent for future cases involving the intersection of antitrust and access to data.

## V. CONCLUSION

The PIPL is a new weapon in the Chinese government's arsenal to reduce or restrict the power of Chinese big tech companies. It should be a very efficient tool given the very restrictive conditions imposed upon the processing of personal data, and the high fines that can be imposed.

While dual enforcement of both the PIPL and the AML is possible, it seems that the PIPL Enforcement Agencies will be better placed to tackle abuses of dominance involving a breach of the PIPL. It remains to be seen whether both enforcement agencies will try to assert their role as the preeminent enforcement agency against Big Tech, which could lead to dual enforcement, or will cooperate and let the better placed agency investigate and put an end to conduct violating both the PIPL and the AML.

One thing is clear, the adoption of the PIPL will have a profound effect on the enforcement of the AML and, as in other jurisdictions, is likely to lead to a significant number of enforcement actions and controversies.

73 It seems that Article 22 of the PIPL, which requires PIH to inform users and obtain their consent in case of a transfer to another PIH, would not apply in the case of a statutory obligation to transfer data because Article 13(7) explicitly provides that consent is not required.

74 Under Article 6.1(c) of the GDPR, data can be processed where it is "necessary for compliance with a legal obligation to which the controller is subject." It is debatable whether this would be a sufficient ground for allowing access to data under Article 102 TFEU (which prohibits abuses of dominance). Indeed, according to recital 41 of the GDPR "*such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it.*" See V. Kathuria & J. Globonick, Exclusionary conduct in data-driven markets: limitation of data sharing remedies, Max Planck Institute for Innovation and Competition, Research paper No. 19-04, p. 23.

75 See above, para. 65.

76 See a summary of the civil lawsuit brought by Eefung Software against Sina Weibo in Chinese at https://www.scmp.com/tech/big-tech/article/3155556/weibo-sued-monopolistic-practices-limiting-access-its-data-chinas.

CPI COMPETITION POLICY™ INTERNATIONAL

# CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.