Antitrust, Vol. 35, No. 1, Fall 2020.

Collingridge Dilemma? The Interaction of Antitrust Law and Data Privacy in China

BY WEI HAN AND CUNZHEN HUANG

THE DIGITAL ECONOMY AND BIG DATA have become the driving force for economic growth globally, including in China. As of March 2020, the number of internet users in China reached 904 million, representing a 64.5 percent penetration rate, of which 897 million were mobile internet users and 99.3 percent used mobile phones to access the internet.[1] In the digital era, data is the new oil, if not more valuable than oil, for fueling products, services, and competition. Meanwhile, calls for more protection for data privacy are on the rise, including by possibly invoking antitrust laws.

The regulators are faced with the Collingridge dilemma. When use of data involving personal sensitive information is still at an early stage of development, it is relatively easier to influence the direction of its development, including by applying antitrust law, but no one knows yet how it would affect the evolution of such data use and society. Yet, when use of such information has become prevalent and its implications are revealed, it might be too late and too difficult to influence its development.

This article summarizes the regulatory framework of China's data privacy protection and its recent enforcement, and details the application of competition-based laws to privacy-related issues. The article concludes by analyzing the potential interaction of antitrust law and data privacy under the Chinese laws.

Regulatory Framework of China Data Privacy Protection

China's regulatory framework for data privacy protection is complex, consisting of numerous laws and regulations that have evolved significantly over recent years.

Wei Han is Associate Professor and Executive Director of the Competition Research Center of the University of Chinese Academy of Social Sciences. Cunzhen Huang is Counsel at Cleary Gottlieb Steen & Hamilton LLP, based in the Washington, DC office. *The authors thank Yiming Sun and Lanxin Chen for their assistance with this article.* *The views expressed in this article are the authors' own and do not necessarily reflect the view of the organizations or institutions they are associated with or the view of their clients.*

Early on, the concept of data privacy was scattered across various laws and policy documents that included varying definitions of personal information, personal data, and electronic information as they relate to data privacy. For example, the Law on Protection of Consumer Rights and Interests, promulgated in 1993 and revised in 2013, specifies the basic requirements for business operators to collect or use personal information. It also clarifies that consumers have rights of personal information protection and stipulates that "business operators that infringe consumers' rights to personal dignity, personal freedom, or personal information shall cease the violations, restore reputation, eliminate effects, and pay compensation."[2]

The Cybersecurity Law, promulgated in 2016, marked a new era of China's data privacy protection. The law provides a comprehensive definition of personal information as "all kinds of information, stored in electronic or other form, which individually or in combination with other information allows the identification of a natural person's individual identity," and enumerates typical forms of personal information, including "a natural person's name, date of birth, identity card number, personally distinctive biological information, address, and telephone number."[3] In addition, the Cybersecurity Law provides basic requirements for network operators in collecting or using personal information. They must abide by the principle of lawfulness, reasonableness, and necessity; explicitly state the rules, purpose, manner, and scope of their collection and use of personal information; and seek the consent of the users. The right of users to ask network operators to delete or correct relevant information of such users under certain circumstances is also provided by the Cybersecurity Law.[4]

The Civil Code, promulgated in May 2020, largely reiterated the definition of personal information and the principles and rules that should be complied with when handling personal data provided in the Cybersecurity Law. It also provided that a "natural person has right to privacy . . . . Privacy is a natural person's right to life tranquility and is private space, private activities, and private information that natural persons do not want to be known by others."[5] It also indicated that the right to privacy only applies to the private information portion of personal data.[6]

In addition, China's regulatory framework comprises many other laws, including the General Provisions of the Civil Law, which classifies the right to personal information as a basic civil right; the Torts Law, which provides liabilities for cyber torts; the E-Commerce Law, which imposes on e-commerce operators duties to protect personal information; and the Ninth Amendments to the Criminal Code, which provides conviction and sentencing standards for criminal offense relating to infringement of citizens' personal information. These laws are supplemented by numerous administrative regulations that set forth principles, methods, and requirements for protecting personal information,[7] as well as rules and other procedural provisions.[8]

In addition, in recent years, the National Administration of Standardization, the National Information Technology Standardization Technical Committee, and the App Special Working Group have published a series of industrial practice guidelines regarding data privacy protection. These rules provide detailed requirements for collecting, processing, storing, sharing, transferring, and deleting personal information and identification of sensitive personal information. They also cover issues arising from the use of new technologies, such as using WIFI beacons and probe requests to collect information; utilizing cookies to collect personal information; and facial recognition technology. These rules include:

- GB/T 35273-2020 Information Technology—Personal Information Security Specification, published by the National Administration of Standardization, which will replace the 2017 version as of October 1, 2020.
- Self-assessment Guidance on Illegal Collection or Uses of Personal Information Through APPs,[9] published by the App Special Working Group.
- Measures for the Ascertainment of Illegal Collection or Uses of Personal Information through APPs.
- Notice on Issuance of Determination Method on Activities of App Illegal Collection of Personal Information, published by Cyberspace Administration of China (CAC) and other departments.[10]

It is worth noting that on October 21, 2020, the draft personal Information Protection Law was published for comment. Once taking effect, this law will become the first law in China that largely focuses on personal information protection.

China Data Privacy Protection Enforcement Practices and Litigation

Administrative Enforcement. Multiple governmental agencies now have responsibility for data privacy protection, including the Ministry of Industry and Information Technology (MIIT), which has historically been the core authority in charge of China's network, and the Cyberspace Administration of China (CAC), which has been taking on an increasingly important role since 2014. Pursuant to the Cybersecurity Law enacted in 2016,[11] the CAC acts as the core authority for overall coordination on network security work and related supervision and management, in cooperation with MIIT (which is responsible for internet access and industry development and promotion) and the Ministry of Public Security (MPS) (which is responsible for, among other things, network registration, network security protection with classification, and internet crime investigation).

In addition, other ministries, including the State Administration of Market Regulation (SAMR), are responsible for relevant matters based on these authorities' designated functions.[12] For example, SAMR established in 2018 after the Chinese government institutional reform, is responsible for the set up of internet enterprises, consumer rights and interests protection, advertisement, and competition compliance. More specifically, within SAMR, the Anti-Monopoly Bureau, the Price Supervision Bureau, the Anti-Unfair Competition Bureau, the Internet Transaction Supervision and Management Committee, and the Law Enforcement Bureau all have the authority to be involved in data privacy issues.

In recent years, CAC, the MIIT, and the MPS (including their local agencies) have stepped up data privacy enforcement. For example, in 2019, four central-level Chinese regulators including the CAC, the MIIT, the MPS, and the SAMR carried out a joint campaign on special app governance. They examined more than 1000 apps' agreement texts, user experiences, and technical details and urged nearly 300 apps with serious problems to rectify their issues.[13] Among other things, the campaign focused on the absence of privacy agreements, unclear description of personal information being collected, collection of personal information beyond the preset scope, and unnecessary collection of personal information.[14] In addition to the joint governance campaign, the MIIT carried out the "special action for telecommunication and internet industry to improve network data security capacity"[15]; the MPB carried out a special campaign, "clean internet 2019"; and the SAMR carried out "protect consumers," a special enforcement action to crack down on violations of consumers' personal information.[16]

Another noteworthy enforcement in 2019 was against an app related to human face recognition. The Chinese tech company Momo Technology developed an extremely popular face-swap app, ZAO, which allowed users to replace themselves with characters in movies and generate a video. ZAO sparked extensive questions from users, and was exposed by media for excessively collecting personal information and allowing unreasonable provisions in its user agreement. For example, according to ZAO's user agreement, after users uploaded their contents, ZAO and its associated companies would be able to edit, modify, and distribute such contents (such as changing the face and voice in the uploaded video to another face and voice). Many users were also particularly concerned that some uploaded contents might be used for facial recognition payment, which has rapidly developed in China.

In September 2019, targeting ZAO's existing issues, such as data leaking risks, the Network Security Bureau under the MIIT carried out an interview with the responsible person from Beijing Momo Technology and requested Momo to carry out self-inspections and take corrective measures, including complying with laws and regulations when collecting users' personal information, modifying user agreements' relevant provisions, and strengthening network data and users' personal information security. After being interviewed by the MIIT, Momo immediately modified its privacy policy and committed to strengthen its content management and improve management mechanisms to ensure user personal information security and data security.[17]

At the beginning of 2020, in the wake of the COVID-19 outbreak, there were violations of citizens' personal privacy in the name of epidemic prevention in China. According to media reports, personal information (such as identification card number, telephone number, home address, information about the train departing from Wuhan) of more than 7,000 Wuhan residents was leaked.[18] In response, in February 2020, the central CAC published the Notice on Utilizing Big Data to Support Joint Prevention and Control Work for Personal Information Protection. The Notice states:

> [P]ersonal information collected for the purpose of epidemic prevention and disease prevention shall not be used for other purposes. Any entities and persons, without consents from the parties whose information are being collected, shall not publicly disclose personal information such as name, age, identification numbers, telephone numbers, and residential addresses. Exceptions will be given to cases where personal information is necessary for joint prevention and control work and sensitive information has been removed.[19]

Judicial Cases. As awareness of data privacy protection has increased, judicial cases have also been filed. One significant case involves the use of facial recognition technology and the uploading (and saving of) user contacts without permission. This lawsuit involves Hangzhou Safari Park's policy of requiring a facial recognition system for entering the park. The plaintiff—a special appointed associate professor—was an annual pass user with the Hangzhou Safari Park, from which he received an SMS message that the park had upgraded its annual pass system to a facial recognition system and discontinued the park's prior fingerprint identification system. The SMS message further noted, "Users cannot enter the park without registrations with the new facial recognition system and cannot get [a] refund for annual pass fees."[20] The plaintiff alleged that biometric data, such as facial recognition information, is classified as personal sensitive information and that the policy violates the Consumers Rights and Interests Protection Law. The plaintiff further alleged that once such type of information is leaked, provided illegally, or was being abused, consumers' physical and property safety will be in a great danger. This lawsuit was lodged in the People's Court in Fuyang Distrcit of Hangzhou and was heard by the court on June 15, 2020. No decision has been handed down at the time of this writing.[21]

Cautious Application of Antitrust Law to Data Privacy Issues in China

Antitrust Enforcement in Matters Involving Data Privacy. With the increasing emergence of data driven business—where the volume, variety, velocity, and value of data are likely to play a critical role in the competitiveness of a business—it is not difficult to understand why there are active discussions about the intersection between antitrust law and data privacy in recent years. This is also true in China, where laws traditionally aimed at promoting competition have data protection components, and competition cases discuss data protection principles.

Before the promulgation of the China Anti-Monopoly Law (AML) in 2007, the Anti-Unfair Competition Law issued in 1993 was widely considered an intended combination of antitrust laws and anti-unfair competition laws—with some consumer protection law touches.[22] However, in recent years, China's Anti-Unfair Competition Law was amended to add, among other things, Article 12, which deals with anti-unfair competition conduct in the internet industry. Although Article 12 does not specifically regulate data privacy, it contains a catch-all clause that specifies that business operators shall not carry out activities that make use of technical means and influence users' choices to hinder or damage network products or services provided by other business operators.

Recent years have seen multiple anti-unfair competition litigations involving data between internet companies. In reality, courts often apply the more abstract Article 2 of the Anti-Unfair Competition Law to try those cases, instead of Article 12, which, as mentioned above, was intended to address issues arising in the internet industry.[23] Despite the catch-all clause in Article 12, Chinese courts may have found that the application of Article 2 may offer more discretion in data privacy cases. The Chinese courts' application of the Anti-Unfair Competition Law to data-related competition cases demonstrates the trend towards more consumer data privacy protection.

For example, in *Sina Weibo v. Maimai*, the court ruled that Maimai's collection and use of information from Sina Weibo users and the acquisition of information regarding the corresponding relationship between Maimai users' contacts and Weibo users, neither of which was consented to by such users or authorized by Weibo, constituted unfair competition.[24] The court established a triple authorization principle consisting of initial user authorization, platform authorization, and user authorization.[25] This principle confirms that an internet platform provider can claim rights and interests in its collected and commercially used users' data as long as these users have given consent to such collection and use. In addition, when a third party (for example,

a third-party platform) tries to use users' information based on a cooperation model, such as Open API, in addition to obtaining consent from the data provider (in this case the internet platform provider), the third party also needs to again obtain consent from the users. This judgment emphasizes respect and protection for users' right of choice and data privacy.

In 2008, the Chinese AML took effect. Like any other antitrust regime, the Chinese AML also aims to protect consumers and promote lower prices, better quality, more choices, and innovation and efficiency. These objectives of competition law can include not only a price dimension but also non-price dimensions, such as quality. In the *Qihu v. Tencent* abuse of dominant position case heard by the Supreme Court in 2014,[26] the court considered the importance of quality competition in the internet industry and pointed out that "Internet service providers tend to pay more attention to competition in quality, service and creativity instead of pricing competition in the Internet industry" and recognized market definition methods such as SSNDQ (small but significant and not-transitory decline of quality).

One could argue that the degree of protection of consumer data privacy is a competition factor of the quality of a product or service, which is directly associated with consumer welfare and constitutes an important non-price competition dimension, particularly in the digital economy (especially with regard to zero-price products). Indeed, China's AML, which has multiple purposes, supports this position. Article 1 of the law provides that "[T]his Law is enacted for the purposes of preventing and restraining monopolistic practices, protecting fair market competition, improving economic efficiency, safeguarding the interests of consumers and the public, and promoting the healthy development of the socialist market economy."[27] Data privacy protection appears to fit in the legislative purposes of "protecting fair market competition" (which covers non-price competition protection) and of safeguarding the interests of consumers.

The implementation rules of the AML, which were updated in 2019 following the 2018 antitrust institutional reform, also contain provisions that touch on data privacy issues—or at least offer the possibility for antitrust enforcement to take data privacy concerns into account.

- Articles 13 and 14 of the AML have, respectively, set forth the types of horizontal and vertical restrictive agreements and both include a catch-all clause ("other restrictive agreements determined by the anti-monopoly authority under the State Council"). The relevant implementing rules, the Interim Provisions on Prohibiting Monopoly Agreement,[28] issued by SAMR in June 2019, clarified several factors SAMR should consider when determining a restrictive agreement, and quality is one of them ("impact of the agreement on price, quantity, and quality and others of the commodity"). As mentioned above, data privacy is an important dimension of quality, particularly when it comes to the quality of a zero-price product. Similar provisions also appear in merger control rules.[29]
- Article 11 of the Interim Provisions on Prohibiting Practices of Abusing Dominant Market Position, issued by SAMR in June 2019, specifies that when determining whether an operator of new economic forms such as the Internet sector holds a dominant market position, the factors considered should include "the ability to hold and handle relevant data."[30] Of course, processing and analyzing voluminous data does not necessarily give rise to a market dominant position, given that such data is non-rivalrous, non-essential, and non-exclusive with diminishing returns.

However, application of competition-related laws in matters involving data privacy issuess is not because of any defect in the data privacy legal system or the need for more data privacy protection in China but because the relevant data privacy issues are relevant to the analysis of competitive effects. For example, privacy competition indicates competitors' willingness to adapt to consumers' desires, consumers' understanding of how their data is being collected and used, and the effectiveness of competition in that relevant market. At present, whether data privacy concerns should be taken into consideration in antitrust analysis is still being heatedly debated. But the AML, flexible implementing rules, and judicial decisions provide the possibility for antitrust enforcement in this area.

Challenges to Quantifying Privacy Competition and Coordination Challenges

It is difficult to evaluate and quantify privacy competition. Traditional antitrust enforcement (including its economic analysis) has developed mature evaluation methods and tools in assessing price competition. In relation to non-price factors, such as quality (in particular privacy), there is still lack of mature and effective assessment tools in most jurisdictions.

Enforcement coordination also brings challenges. SAMR, newly established in 2018, is a regulatory agency with a wide range of responsibilities, including antitrust enforcement. The Anti-Monopoly Bureau, as one of SAMR's departments, may need to coordinate with several other departments of SAMR, including the Price Supervision Bureau and the Anti-Unfair Competition Bureau,[31] the Online Transaction Supervision and Management department,[32] and the Law Enforcement Inspection Bureau,[33] when handling competition matters that involve data privacy. External coordination outside SAMR may also be required, for example, with CAC and MIIT. However, protracted antitrust investigation timelines and more unpredictable enforcement outcomes may result from the need for inter-departmental and inter-agency coordination.

Conclusion and Outlook

The current data privacy protection legal framework is large, complex, and scattered. It needs time to mature.

However, this complex system is not a reason for using antitrust law to tackle increasing concerns about privacy in the rapidly developing digital economy. Nonetheless, privacy is one dimension of quality competition, and thus while the best-calibrated role for antitrust law to take in resolving competition issues arising from data privacy is not yet clear, it does have a role to play. ■

[1] The Office of the Central Cyberspace Affairs Commission, The Cyberspace Administration of China, The 45th China Statistical Report on Internet Development (2020), http://www.cac.gov.cn/2020-04/27/c_1589535470378587.htm.

[2] Law on Protection of Consumer Rights and Interests art. 50 (2019), http://gkml.samr.gov.cn/nsjg/fgs/201906/t20190625_302783.html.

[3] Cybersecurity Law art. 76 (5) (2016), http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

[4] *Id.* arts. 40–45.

[5] The Civil Code arts. 1032 and 1034 (2020), http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml.

[6] *Id.* ch. 6, http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml.

[7] Examples of these regulations include: the Regulation on Telecommunications, the Regulation on Internet Information Service, the Interim Regulation on Residence Permits, the Regulation on Map Management, and the Regulation on the Administration of Credit Investigation Industry.

[8] Examples include: the Provisions on Protecting the Personal Information of Telecommunications and Internet Users, the Provisions on the Cyber Protection of Children's Personal Information, the Provisions on the Administration of Programs for Minors, the Provisions on the Administration of Financial Information Services, the Provisions on the Administration of Cyber Audio and Video Information Services, the Management Measures on National Standards, Security and Service of Big Data in Health and Medical Care (Trial), the Guide on Internet Personal Information Security Protection, the Cybersecurity Review Measures, and the Means for Determination of Violations of Laws and Regulations in Apps' Collection and Use of Personal Information.

[9] Personal Information Protection Task Force on Apps, Self-Assessment Guidelines on App Illegal Collection of Personal Information (2019), http://pip.tc260.org.cn/jbxt/privacy/detail/20190302114600934277.

[10] Cyberspace Administration of China (CAC), the Notice on Issuance of Determination Method on Activities of App Illegal Collection of Personal Information (2019), http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm.

[11] Article 8 of the Cybersecurity Law stipulates that "the CAC is responsible for overall coordination on network security work and related supervision and management. State Council telecommunication administration, public security administration, and other relevant authorities shall be responsible for network security protection and supervision and management work within its respective scope of responsibilities following this law and other relevant regulations and administrative regulations." *See* Cybersecurity Law art. 8 (2016), http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

[12] For example, the game industry is under the Central Propaganda Department's competence; visual and audio programs are under the State Administration of Radio, Film and Television's competence; internet, entertainment, and music are under the Ministry of Culture and Tourism's competence; and internet finance is under the People's Bank of China and other finance authorities' competence.

[13] CAC, Joint Campaign on Special App Governance Carried Out Jointly by CAC, MIIT, MPS, and SAMR (2019), http://www.cac.gov.cn/2019-01/25/c_1124042585.htm.

[14] Jiang Lin, *Special App Governance: Urge 300 Apps To Take Corrective Measures and SAMR's Plan To Issue First Batch of App Safety Certificates* (2019), https://www.sohu.com/a/363626474_161795.

[15] MIIT, *Special Action on Improving Network Data Security and Protection Ability for Telecommunication and Internet Industry* (2019), http://www.miit.gov.cn/n1146290/n1146402/n1146440/c7116222/content.html.

[16] News Release, SAMR, Carrying Out Special Enforcement Action on Cracking Down Illegal Activities Against Infringements of Consumers' Personal Information (2019), http://www.gov.cn/xinwen/2019-04/11/content_5381525.htm.

[17] Zhang Honglei, *ZAO App Accused of Data Leaking Risks and Interviewed by MIIT* (2019), https://baijiahao.baidu.com/s?id=1643762209561054968&wfr=spider&for=pc.

[18] Li Huiqi, Li Ling & Song Chenghan, *Over 7000 Wuhan Returnees' Personal Information Leaked and They Were Harassed and Abused Through Text Messages* (2020) , https://view.inews.qq.com/w2/20200127A092N900?tbkt=E&strategy=&openid=o04IBAAATe3gwuMDx8xnxTTf-x44&uid=&refer=wx_hot.

[19] CAC, the Notice on Using Big Data to Support Joint Prevention and Control and Protection of Personal Information (2020), http://www.cac.gov.cn/2020-02/09/c_1582791585580220.htm.

[20] Zhao Kaidi, *The First Facial Recognition Case in China: Zoo Sued at Court for Launching Facial Recognition Tech* (2019), http://news.ifeng.com/c/7rHNBE5VpuA.

[21] Ren Huafei, *China's First Facial Recognition Case Heard at Court Today but Decision Not Made During Court Sessions* (2019), http://www.dahebao.cn/news/1544277?cid=1544277.

[22] Among the 11 categories of prohibited conducts clearly defined in the 1993 Anti-Unfair Competition Law, five were better governed by antitrust laws. Those five categories of conduct that eliminate or restrict competition in the sense of antitrust law were deleted from the amended law.

[23] Clause 2 of Article 2 of the new Anti-Unfair Competition Law of the People's Republic of China stipulates that "[f]or the purpose of this Law, unfair competition refers to any business operator's act of participating in the production and operation activities in violation of the provisions herein to disrupt the competition order in the market and infringe the legitimate rights and interests of other business operators or consumers." *See* The Anti-Unfair Competition Law, art. 2 (2) (2019), http://gkml.samr.gov.cn/nsjg/fgs/201906/t20190625_302771.html.

[24] She Yin, Sina Weibo v. Maimai, *the First Unfair Competition Case Caused by Big Data* (2017), http://news.sina.com.cn/sf/news/ajjj/2017-02-08/doc-ifyafenm3035943.shtml.

[25] Zhang Lingling, *Application of Article 2 of the Anti-Unfair Competition Law Illustrated by the* Case Sina Weibo v. Maimai (2017), http://www.sohu.com/a/165122267_455313.

[26] *See* Qihu v. Tencent, The Supreme Court of the Peoples' Republic of China, Civil Judgment ((2013) Min San Zhong Zi No. 4), https://cgc.law.stanford.edu/zh-hans/judgments/spc-2013-min-san-zhongzi-4-civil-judgment/.

[27] Anti-Monopoly Law, art. 1 (2007), http://www.gov.cn/flfg/2007-08/30/content_732591.htm.

[28] SAMR, the Interim Provisions on Prohibiting Monopoly Agreement (2019), http://gkml.samr.gov.cn/nsjg/fldj/201907/t20190725_305165.html.

[29] *See* MOFCOM, Interim Provisions on Evaluating the Impact of Concentration of Business Operators on Competition art. 9 (2011), http://www.gov.cn/zwgk/2011-09/02/content_1939083.html; *see also* SAMR, Interim Provisions on Review of Concentration of Business Operators (Draft for Comment) art. 37 (2020), http://www.samr.gov.cn/hd/zjdc/202001/t20200107_310318.html.

[30] SAMR, the Interim Provisions on Prohibiting Practices of Abusing Dominant Market Position art. 11 (2019), http://gkml.samr.gov.cn/nsjg/fldj/201907/t20190725_305166.html.

[31] *See* Price Supervision and Inspection Bureau and the Anti-unfair Competition Bureau, http://www.samr.gov.cn/jjj/index.html.

[32] *See* Online Transaction Supervision and Management Department, http://www.samr.gov.cn/wljys/.

[33] *See* Law Enforcement Inspection Bureau, http://www.samr.gov.cn/zfjcj/.