THE ROLE OF COMPETITION LAW IN REGULATING DATA IN CHINA'S DIGITAL ECONOMY

WENDY NG*

As the importance of digital markets to society has grown, so too has the volume and variety of data that have been generated, collected, used, and shared. Increasingly, the ability to access, control, analyze, and apply data is a source of competitive advantage for businesses, especially those operating in the digital economy. At the same time, the data and data practices of businesses have come under regulatory and political scrutiny. In the United States, for example, the data practices of TikTok, owned by ByteDance, a Chinese company, came under intense political and public scrutiny over concerns that user information was being shared with and accessed by the Chinese government, raising questions relating to privacy, data security, cybersecurity, and national security.[1]

Similarly, data and data practices are key concerns in competition law discussions surrounding the regulation of digital platforms.[2] Questions such as how data affect market definition and the assessment of market power and competitive effect, when data-based business strategies and practices might constitute anticompetitive conduct, and whether privacy and data protection matters should be incorporated into competition law frameworks are being discussed and debated by competition regulators and legislators all around the world.[3] Germany's Bundeskartellamt handed down a landmark decision in

* Associate Professor, Melbourne Law School, The University of Melbourne. I would like to thank Eleanor Fox, Michal Gal, Yee Wah Chin, Su Sun, Angela Zhang, and the anonymous reviewers for their helpful comments on earlier versions of this article.

[1] *See, e.g.*, David McCabe, *What's Going on with TikTok? Here's What We Know*, N.Y. TIMES (Aug. 3, 2020); Bowdeya Tweh & Euirim Choi, *Does Oracle's Winning Bid for TikTok's U.S. Operations Avert a Ban?*, WALL ST. J. (Sept. 13, 2020); Samm Sacks, *Banning TikTok Is a Terrible Idea*, SUPCHINA (July 16, 2020), supchina.com/2020/07/16/banning-tiktok-is-a-terrible-idea.

[2] *See, e.g.*, Filippo Lancieri & Patricia Morita Sakowski, *Competition in Digital Markets: A Review of Expert Reports*, 26 STAN. J.L. BUS. & FIN. 65, 65–66 (2021).

[3] *See, e.g.*, Press Release, INTERNATIONAL COMPETITION NETWORK, Intersection of Competition, Consumer Protection, & Privacy—September 7 (Sept. 3, 2021), www.internationalcompetitionnetwork.org/news-events/intersection-sept2021/; AUSTRL. COMPETITION & CONSUMER

February 2019, when it found that Facebook had breached German competition laws for its collection, processing, and use of user and device-related data.[4] This is the first decision made by a competition authority that has based a breach of competition law on a violation of privacy and data protection laws. Data and data practices have also been targeted in competition law and related legislative reforms that have been adopted, or are being considered, that provide for ex ante regulation of digital platforms.[5]

The data and data practices of companies are also attracting political and regulatory attention in China. Over the past few years, China has been developing a legal regime to regulate and enable the state to exercise control over data, covering matters relating to cybersecurity, data security, and personal information protection. Moreover, after a long period of relatively lax regulatory oversight and control over internet and technology companies that tended to favor innovation and growth over regulation, China has now shifted to tighten regulatory scrutiny and control over these companies, and the sector more broadly.[6] The suspension of the much-anticipated initial public offering of Ant Group (a subsidiary of Alibaba operating in the financial technology sector) in November 2020 by the Shanghai Stock Exchange less than 48 hours before its securities were scheduled to start trading[7] was the watershed mo-

---

COMM'N, DIGITAL PLATFORMS INQUIRY: FINAL REPORT (2019); JAPAN FAIR TRADE COMM'N, REPORT REGARDING TRADE PRACTICES ON DIGITAL PLATFORMS: BUSINESS-TO-BUSINESS TRANSACTIONS ON ONLINE RETAIL PLATFORMS AND APP STORES (2019); SUBCOMM. ON ANTITRUST, COM., AND ADMIN. LAW OF THE H. COMM. ON THE JUDICIARY, 116TH CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS: MAJORITY STAFF REPORT AND RECOMMENDATIONS (2020); AUSTRL. COMPETITION & CONSUMER COMM'N, DIGITAL PLATFORM SERVICES INQUIRY: DISCUSSION PAPER FOR INTERIM REPORT NO. 5 (2022).

[4] B6-22/16—Facebook Inc. (Social Networks), Bundeskartellamt [BKartA] [Fed. Cartel Off.] Decision (Feb. 6, 2019), www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3591568. This decision was appealed by Facebook and, at the time of writing this article, the appeal is ongoing.

[5] Examples of such legislative reforms include the 10th Amendment to Germany's Act Against Restraints of Competition that came into effect in January 2021 and the European Union's Digital Markets Act, the text of which was provisionally agreed to by the European Parliament and the European Council in March 2022. *See* Gesetz gegen Wettbewerbsbeschränkungen [GWB] [Competition Act], June 26, 2013, BGBl I, last amended by Gesetz [G], July 9, 2021, BGBl I., www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html; Eur. Comm'n, *Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)*, COM (2020) 842 final (Dec. 15, 2020).

[6] *See, e.g.*, Angela Huyue Zhang, *Agility over Stability: China's Great Reversal in Regulating the Platform Economy*, 63 HARV. INT'L L.J. (forthcoming Nov. 2022).

[7] Zhongguo Renmin Yinhang Fuxingzhang Pan Gongsheng Jiu Jinrong Guanli Bumen Yuetan Mayi Jituan Youguan Qingkuang Da Jizhe Wen (中国人民银行副行长潘功胜就金融管理部门约谈蚂蚁集团有关情况答记者问) [Pan Gongsheng, Deputy Governor of the People's Bank of China, Answered Reporters' Questions about the Financial Management Department's Interview with Ant Group], THE PEOPLE'S BANK OF CHINA (Dec. 27, 2020), www.pbc.gov.cn/goutongjiaoliu/113456/113469/4153479/index.html; Raymond Zhong & Cao Li, *China Halts Ant Group's Blockbuster I.P.O.*, N.Y. TIMES (Nov. 3, 2020); John Liu et al., *Ant IPO Has Slim Chance of Getting Done Next Year*, BLOOMBERG NEWS (Nov. 29, 2020); Chad

ment that shifted political and regulatory attitudes towards big internet and technology companies operating in China, and the sector more generally. Not only did the Chinese government take a series of regulatory interventions and measures[8] to discipline Alibaba, one of the largest and most high-profile internet conglomerate companies in China, it also began a multi-pronged regulatory and enforcement campaign targeting the internet and technology sector. Chinese regulators have taken actions against specific companies and adopted a raft of new regulations to govern the activities of businesses operating in the digital economy. This campaign has covered a diverse range of areas and concerns, including, *inter alia*, data, financial regulation, cybersecurity, labor, transportation, online gaming, online education, fan culture, and wealth redistribution.[9] Competition law, in particular, has played a conspicuous role in this campaign.

This article examines whether and how China's competition laws might apply to regulate the data and data practices of businesses operating in the digital economy. It does so by undertaking a political economy and contextual exploration of China's data regulatory environment and its relationship and interaction with China's competition laws. The nature of China's political economy, as well as of its competition laws, means that a variety of interests, goals, and priorities—which might encompass concerns that other jurisdictions might regard as being beyond the purview of competition law—are considered and balanced in the enforcement of competition law, under the macroeconomic supervision and guidance of the state.

This article is structured as follows. Part I examines China's data regulatory environment. In addition to analyzing the legal framework that has been developed to regulate data, this Part also draws out the interests, concerns, and goals that the state, businesses, and individuals have in data. It also discusses the other avenues the state uses to influence the predominantly private internet and technology companies that operate in China and looks at the political dynamics of data governance. Part II examines how China's competition laws

---

Bray, *Ant Group IPO Resumption Will Depend on How Company Adapts to New Fintech Rules, CSRC Official Says*, S. CHINA MORNING POST (Nov. 17, 2020); Jing Yang & Lingling Wei, *China's President Xi Jinping Personally Scuttled Jack Ma's Ant IPO*, WALL ST. J. (Nov. 12, 2020).

[8] Raymond Zhong, *Ant Group Announces Overhaul as China Tightens Its Grip*, N.Y. TIMES (Apr. 12, 2021); Jing Yang, *Tencent Faces Possible Record Fine for Anti-Money-Laundering Violations*, WALL ST. J. (Mar. 14, 2022).

[9] *See, e.g.*, Stephanie Yang, *China's Tech Clampdown Is Spreading Like Wildfire*, WALL ST. J. (June 6, 2021); Li Yuan, *What China Expects from Businesses: Total Surrender*, N.Y. TIMES (Oct. 8, 2021); Chang Che & Jeremy Goldkorn, *China's 'Big Tech Crackdown': A Guide*, SUPCHINA (Aug. 2, 2021), supchina.com/2021/08/02/chinas-big-tech-crackdown-a-guide; Jing Yang et al., *China's Corporate Crackdown Is Just Getting Started. Signs Point to More Tumult Ahead*, WALL ST. J. (Aug. 5, 2021); Lingling Wei, *China's New Power Play: More Control of Tech Companies' Troves of Data*, WALL ST. J. (June 12, 2021).

are being applied to regulate the data and data practices of businesses. This article then explores the relationship between China's data governance regime and competition laws and how that might influence the application of the competition laws in Part III. Part IV concludes.

I. CHINA'S DATA REGULATORY ENVIRONMENT

The collection, access, use, transfer, and sharing of data are regulated, monitored, and controlled by the Chinese government in a variety of ways. In doing so, the state is trying to balance the commercial interests of the businesses that are collecting and handling that data, the privacy interests of the individuals who provide that data, and its own interests in data.

This Part first provides an overview of the state's various interests in and concerns over data. It then sets out and analyzes the current legal framework for data governance, drawing out in particular how it balances, pursues, and addresses multiple concerns, goals, and interests that individuals, businesses, and the state have in data. Beyond the data governance laws, the state uses other formal and informal means to exercise control and influence over the private companies that dominate the digital economy, which are also discussed. Finally, this Part considers some of the political dynamics and considerations that arise in data governance. It is noted that, while China's approach to data governance may have significant consequences beyond its national borders,[10] such considerations are beyond the scope of this article.

A. THE STATE'S INTERESTS IN DATA

In China, data are viewed both in terms of the opportunities they present, as well as the risks that they pose, and this view shapes the way that the state approaches data governance. Data are relevant to the state's national security,[11] public security, and economic and social development goals and interests. Moreover, the introduction, development, and proliferation of the internet—and with it, the expansion of the ways in which information may be

---

[10] *See, e.g.*, Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, 54 N.Y.U. J. INT'L L. & POL. 1 (2021); Zhang Xiaosong & Zhu Jichai, *Xi Jinping: Independent Innovation Promotes the Establishment of a Cyber Superpower*, XINHUA (Apr. 21, 2018), www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm; Samantha Hoffman, *Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion* (Austrl. Strategic Pol'y Inst. Int'l Cyber Pol'y Ctr., Rep. No. 21, 2019).

[11] National security is a concept that encompasses political, homeland, military, economic, cultural, societal, technological, information, ecological, resource, and nuclear security, and there is express recognition that development and security go hand-in-hand: *Xi Jinping: Jianchi Zongti Guojia Anquan Guan, Zou Zhongguo Tese Guojia Anquan Daolu* (习近平: 坚持总体国家安全观 走中国特色国家安全道路) [Xi Jinping: Adhere to the Complete View of National Security, Follow the Path of National Security with Chinese Characteristics], XINHUA (新华) (Apr. 15, 2014), www.xinhuanet.com//politics/2014-04/15/c_1110253910.htm.

accessed, shared, and communicated, the growing digital economy, and generation of huge volumes of data—have also influenced the state's approach to data and its regulation. In particular, internet regulation has become integrally entwined with data regulation.[12]

China looks at data through a political and national security lens. The state has long controlled information and its avenues of dissemination to prevent political instability. It proactively censors and regulates media content, owns traditional media outlets, and regulates media and other publication outlets. China also has a powerful propaganda system and engages in proactive propaganda activities—that is, it creates and distributes information that it believes should be known by the public.[13] The internet has amplified the political, national security, and sovereignty aspects of data because the internet has made it easier for people to access and communicate information, which poses a new challenge and risk to state power.[14] As such, the internet has become an indispensable aspect of China's national security and sovereignty,[15] and the state uses various technological and regulatory means to monitor, control, filter, and censor the information that people can access and disseminate online, the avenues through which such information can be accessed and distributed, and other online activities.[16]

At the same time, data are important to China's economic and development goals.[17] In particular, the state views data as economic assets. Data are treated

---

[12] Henry S. Gao, *Data Regulation with Chinese Characteristics*, *in* BIG DATA AND GLOBAL TRADE LAW 245, 261 (Mira Burri ed., 2021).

[13] *See generally* David Shambaugh, *China's Propaganda System: Institutions, Processes and Efficacy*, 57 CHINA J. 25 (2007); Austin Jun Luo, *Media System in China: A Chinese Perspective*, 2 INT'L COMMC'N CHINESE CULTURE 49 (2015).

[14] Rogier Creemers, *Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century*, 26 J. CONTEMP. CHINA 85, 86–87 (2017); Lokman Tsui, *The Panopticon as the Antithesis of a Space of Freedom: Control and Regulation of the Internet in China*, CHINA INFO., Oct. 2003, at 65; Elizabeth C. Economy, *The Great Firewall of China: Xi Jinping's Internet Shutdown*, THE GUARDIAN (June 29, 2018).

[15] Xi Jinping, Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference (Dec. 16, 2015), www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html; Zhang & Zhu, *supra* note 10; INFORMATION OFFICE OF THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA, THE INTERNET IN CHINA (2010).

[16] *See, e.g.*, Sebastian Heilmann, *Big Data Reshapes China's Approach to Governance*, FIN. TIMES. (Sept. 28, 2017); Min Jiang & King-Wa Fu, Editorial, *Chinese Social Media and Big Data: Big Data, Big Brother, Big Profit?*, 10 POL'Y & INTERNET 372, 378–83 (2018); Lotus Ruan, *When the Winner Takes It All: Big Data in China and the Battle for Privacy* 5–7 (Austrl. Strategic Pol'y Inst. Int'l Cyber Pol'y Ctr., Rep. No. 5, 2018).

[17] *See, e.g.*, Guomin Jingji He Shehui Fazhan Di Shisi Ge Wunian Guihua He 2035 Nian Yuanjing Mubiao Gangyao (国民经济和社会发展第十四个五年规划和2035年远景目标纲要) [Outline of the 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035] (promulgated by the Nat'l. People's Cong., Mar. 11, 2021) (China), ch. 15, ch. 28 art. 1 [hereinafter Outline of the 14th Five-Year Plan].

as factors of production, and the development of a data factor market is essential to ensuring high-quality development.[18] Similarly, big data are viewed as fundamental strategic resources,[19] and not only is there a range of policies to facilitate the development of big data industries,[20] many of China's key development strategies rely on big data-driven solutions.[21] Data are also key inputs into China's informatization strategy, which is the transformation of an economy, society, and governance into one that is driven by information technology.[22] Further, the state is increasingly harnessing data to support and transform its state functions, such as policing, surveillance, social control, and delivery of government services.[23] For example, China is developing measures relating to "social credit," whereby technology and digital data are used and integrated with the aim of improving economic and social order and trust between people,[24] and it is strengthening the sharing of data between govern-

---

[18] Guanyu Goujian Gengjia Wanshan De Yaosu Shichang Hua Peizhi Tizhi Jizhi De Yijian (关于构建更加完善的要素市场化配置体制机制的意见) [Opinions on Constructing a More Perfect Market-Based Allocation Mechanism for Production Factors] (promulgated by the Cent. Comm. Chinese Communist Party and State Council, Mar. 30, 2020) (China), ch. 6.

[19] Guomin Jingji He Shehui Fazhan Di Shisan Ge Wunian Guihua Gangyao (国民经济和社会发展第十三个五年规划纲要) [Outline of the 13th Five-Year Plan for National Economic and Social Development] (promulgated by the Nat'l. People's Cong., Mar. 17, 2016) (China), ch. 27.

[20] Cujin Dashuju Fazhan Xingdong Gangyao (促进大数据发展行动纲要) [Outline of the Plan to Promote the Development of Big Data] (promulgated by the State Council, Sept. 5, 2015) (China); Zhongguo Zhizao (中国制造) [Made in China 2025] (promulgated by the State Council, May 8, 2015) (China); Jiji Tuijin "Hulianwang+" Xingdong De Zhidao Yijian (积极推进"互联网+"行动的指导意见) [Guiding Opinions on Actively Promoting "Internet Plus" Action Plan] (promulgated by the State Council, July 4, 2015) (China); Outline of the 14th Five-Year Plan, *supra* note 17, ch. 15 tbl.8.

[21] Heilmann, *supra* note 16.

[22] 2006–2020 Nian Guojia Xinxi Hua Fazhan Zhanlüe (2006-2020 年国家信息化发展战略) [2006–2020 National Informatization Development Strategy] (promulgated by the Cent. Comm. Chinese Communist Party and State Council, Mar. 19, 2006) www.gov.cn/gongbao/content/2006/content_315999.htm (China); Guojia Xinxi Hua Fazhan Zhanlüe Gangyao (国家信息化发展战略纲要) [Outline for the National Informatization Development Strategy] (promulgated by the Cent. Comm. Chinese Communist Party Gen. Office and State Council Gen. Office, July 27, 2016) (China); "Shisi Wu" Guojia Xinxi Hua Guihua ("十四五" 国家信息化规划) [14th Five-Year Plan for National Informatization] (promulgated by the Cent. Cybersecurity and Informatization Comm., Dec. 28, 2021) (China). *See also* Nagy K. Hanna & Christine Zhen-Wei Qiang, *China's Evolving Informatization Strategy*, *in* SEEKING TRANSFORMATION THROUGH INFORMATION TECHNOLOGY: STRATEGIES FOR BRAZIL, CHINA, CANADA AND SRI LANKA 89 (Nagy K. Hanna & Peter T. Knight eds., 2011).

[23] Outline of the 14th Five-Year Plan, *supra* note 17, ch. 17 art. 1. *See also* Severine Arsene, *Tech Giants' Agenda Is at Odds with CCP Priorities*, ASIA DIALOGUE (Sept. 6, 2018), theasiadialogue.com/2018/09/06/chinas-digital-dilemmas; Yang Feng, *The Future of China's Personal Data Protection Law: Challenges and Prospects*, 27 ASIA PAC. L. REV. 62, 67 (2019).

[24] Shehui Xinyong Tixi Jianshe Guihua Gangyao (2014–2020) (社会信用体系建设规划纲要) [Outline for the Development of a Social Credit System (2014–2020)] (promulgated by the State Council, June 14, 2014) (China). *See, e.g.*, Jeremy Daum, *China Through a Glass, Darkly*, CHINA LAW TRANSLATE (Dec. 24, 2017), www.chinalawtranslate.com/en/china-social-credit-score; Xin Dai, *Toward a Reputation State: A Comprehensive View of China's Social Credit*

ment departments and digital platforms to help it to collect market and business information and carry out e-government functions.[25]

B. LEGAL FRAMEWORK FOR DATA REGULATION

At the time of writing, the principal laws regulating data in China are the Cybersecurity Law,[26] the Data Security Law,[27] and the Personal Information Protection Law.[28] These laws are the key pillars of China's legal framework for data regulation.[29]

The three laws approach the regulation of data from different perspectives that are consistent with the state's own interests in data as well as the commercial interests of businesses and privacy interests of individuals. The Cybersecurity Law regulates data to ensure cyber and national security; to protect cyber sovereignty, the social and public interests, and the legitimate rights of citizens, legal persons, and other organizations; and to promote the healthy development of the informatization of the economy and society.[30] The Data Security Law likewise regulates data under the rubric of safeguarding sovereignty and national and public security, developing data and data-related industries and technologies and the digital economy, and protecting the data rights and interests of individuals and organizations.[31] The Personal Information Protection Law primarily aims to protect the rights and interests of individuals in personal information.[32] Relatedly, the type of data regulated by each law is also different. The scope of the Data Security Law is the broadest, as it applies to any information record (whether in electronic or other form),[33]

System Project, *in* SOCIAL CREDIT RATING: REPUTATION UND VERTRAUEN BEURTEILEN 139 (Oliver Everling ed., 2020).

[25] Cujin Pingtai Jingji Guifan Jiankang Fazhan De Zhidao Yijian (促进平台经济规范健康发展的指导意见) [Guiding Opinions on Promoting the Orderly and Healthy Development of the Platform Economy] (promulgated by the State Council, Aug. 1, 2019) (China), ¶ 4.

[26] Wangluo Anquan Fa (网络安全法) [Cybersecurity Law] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017) (China).

[27] Shuju Anquan Fa (数据安全法) [Data Security Law] (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021) (China).

[28] Geren Xinxi Anquan Baohu Fa (个人信息安全保护法) [Personal Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) (China).

[29] For a history of the development of China's data governance legal framework, see Rogier Creemers, *China's Emerging Data Protection Framework* (Nov. 16, 2021) (unpublished manuscript), ssrn.com/abstract=3964684.

[30] Cybersecurity Law (China), *supra* note 26, art. 1; *id.* arts. 1–3.

[31] Data Security Law (China), *supra* note 27, arts. 1, 4, 7, 8.

[32] Personal Information Protection Law (China), *supra* note 28, arts. 1, 11. *See also* Explanation of the Personal Information Protection Law (Draft) (Standing Comm. Nat'l People's Cong. Legis. Aff. Comm'n, Oct. 31, 2020).

[33] State secrets and military data are excluded from the scope of the Data Security Law. Data Security Law (China), *supra* note 27, arts. 53–54.

whereas the Cybersecurity Law regulates network data[34] and personal information and the Personal Information Protection Law applies to personal information only.

Overall, the data governance regime focuses on the duties of businesses and, to a lesser extent, state authorities[35] with respect to data. These obligations fall into several broad categories. First, most of these obligations relate to ensuring the security of data from a systems and operations perspective. Businesses are required to implement data security management systems, and those that are "important data" handlers must conduct periodic risk assessments of their data handling activities[36] and designate specific persons and management bodies to be responsible for carrying out their data security obligations.[37] Network operators[38] are required to adopt certain measures to prevent network data from being leaked, stolen, and falsified.[39] Operators of critical information infrastructure[40] must also ensure the operations security of those networks[41] and store network data that is important data or personal information within China.[42] Similarly, state authorities are required to establish data security management systems, implement data security protection responsibilities, and ensure the security of government data.[43] Second, individuals and organizations are subject to some prohibitions. They must not steal or otherwise unlawfully obtain data[44] or provide data stored within China to judicial or law enforcement institutions of foreign countries without ob-

---

[34] Network data are electronic data that is collected, stored, transmitted, processed, and produced through computer networks. Cybersecurity Law (China), *supra* note 26, art. 76(4).

[35] Under the Cybersecurity Law, Article 45 applies to departments responsible for cybersecurity supervision and management, and Article 30 applies to departments responsible for cybersecurity and informatization and cybersecurity protection. Under the Data Security Law, Article 38 applies to state authorities and other organizations that are authorized by law to carry out public affairs management duties. Under the Personal Information Protection Law, Article 37 provides that the obligations imposed on state organs also apply to organizations that are authorized by law to carry out public affairs management duties. *See* Cybersecurity Law (China), *supra* note 26, arts. 30, 45; Data Security Law (China), *supra* note 27, art. 38; Personal Information Protection Law (China), *supra* note 28, art. 37.

[36] Data Security Law (China), *supra* note 27, art. 30.

[37] *Id.* art. 27.

[38] "[R]efers to network owners, [network] managers, and network service providers." Cybersecurity Law (China), *supra* note 26, art. 76(3).

[39] *Id.* art. 21.

[40] Critical information infrastructure includes "public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which . . . might seriously endanger national security, national welfare, the people's livelihood, or the public interest" if it is destroyed, suffers a loss of function, or experiences data leakage. *Id.* art. 31.

[41] *Id.* arts. 31–39; Data Security Law (China), *supra* note 27, arts. 27, 29.

[42] Cybersecurity Law (China), *supra* note 26, art. 37.

[43] Data Security Law (China), *supra* note 27, art. 39.

[44] Cybersecurity Law (China), *supra* note 26, art. 27; *id.* art. 32.

taining government approval.[45] Third, businesses are required to provide assistance to and cooperate with public security and national security authorities, cybersecurity and informatization departments, government departments carrying out personal information protection duties, and other relevant government departments that engage in supervision and inspection activities. This means, as part of that cooperation and assistance, businesses might need to provide their data to government authorities.[46]

The data governance regime also distinguishes between different types of data. Data are categorized based on their importance to economic and social development and their risk to national security, public interests, and the lawful rights of individuals and organizations if those data are changed, destroyed, leaked, or unlawfully obtained or used.[47] In particular, data will constitute the "core data of the state" if they relate to national security, the lifeline of the national economy, important aspects of people's livelihoods, and major public interests.[48] The categorization of data affects the level of protection that data are afforded, how data are managed, and whether data are subject to data localization and outbound security management rules. For example, core data of the state are subject to a stricter management system,[49] and network data that are classified as "important data" have stronger protections,[50] need to be stored within China,[51] and are subject to outbound security management measures.[52]

In particular, personal information is subject to additional restrictions, protections, and regulation under the data regulatory regime. The way that personal information is addressed by the data governance laws is characterized by three key features. First, personal information is regulated and protected in a manner that recognizes its value to both individuals and the state. The Personal Information Protection Law and the Cybersecurity Law provide individuals with some degree of control over and protection of their personal information. Individuals must consent to the collection, use, and handling of

---

[45] Data Security Law (China), *supra* note 27, art. 36.

[46] Cybersecurity Law (China), *supra* note 26, arts. 28, 49; *id*. art. 35; Personal Information Protection Law (China), *supra* note 28, art. 63.

[47] Data Security Law (China), *supra* note 27, art. 21.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] Cybersecurity Law (China), *supra* note 26, art. 37.

[52] Data Security Law (China), *supra* note 27, art. 31. In October 2021 the Cyberspace Administration of China released draft measures relating to security assessment for cross-border data transfers: Shuju Chujing Anquan Pinggu Banfa (Zhengqiu Yijian Gao) (数据出境安全评估办法 (征求意见稿)) [Measures on Security Assessments for Exporting Data (Draft for Comment)] (released by the Cyberspace Admin. of China, Oct. 29, 2021) (China).

their personal information, which can be rescinded and withdrawn.[53] They can also access and copy their personal information and request that their personal information be transferred to another handler, that errors in their personal information be corrected, and that unlawfully obtained or handled personal information be deleted.[54] Sensitive personal information[55] is also afforded more protection and subject to greater restrictions than other types of personal information.[56] Further, where automated decision-making is used and has a major effect on an individual's rights and interests, individuals have the right to request an explanation from the business for the decision and the right to refuse to have that decision be made by automated decision-making means.[57] At the same time, personal information is protected under the Cybersecurity Law because it is an important aspect of ensuring network information security.[58] There are also restrictions on transferring personal information to locations outside of China, and some businesses[59] and state authorities must store the personal information that they collect and handle within China.[60]

Second, businesses play critical roles in regulating personal information. They are the primary source of personal information protection for individuals because the data governance laws are aimed largely at addressing the commercial risks associated with the collection, use, and handling of personal information. Businesses are required to obtain consent to collect, use, and handle personal information,[61] provide individuals with certain information before handling their personal information,[62] and use technological and other means to ensure information security and prevent the unauthorized access,

---

[53] Cybersecurity Law (China), *supra* note 26, arts. 41–42; Personal Information Protection Law (China), *supra* note 28, arts. 13–15, 23.

[54] Cybersecurity Law (China), *supra* note 26, art. 43; Personal Information Protection Law (China), *supra* note 28, arts. 45–47.

[55] Sensitive personal information is "personal information that, if leaked or unlawfully used, can easily lead to the harm of a natural person's personal dignity or personal or property security. This includes biometric information, religious beliefs, specific identities, medical health, financial accounts, location tracking, and the personal information of minors under the age of 14." Personal Information Protection Law (China), *supra* note 28, art. 28.

[56] *Id.* arts. 28–29, 31.

[57] *Id.* art. 24.

[58] *See* Cybersecurity Law (China), *supra* note 26, ch. 4.

[59] Critical information infrastructure operators that collect or produce personal information in China or businesses that handle personal information reaching volumes as specified by the State cybersecurity and informatization department. *See id.* art. 37; Personal Information Protection Law (China), *supra* note 28, art. 40.

[60] Cybersecurity Law (China), *supra* note 26, art. 37; Personal Information Protection Law (China), *supra* note 28, art. 36. *See also* Measures on Security Assessments for Exporting Data (Draft for Comment) (China).

[61] Cybersecurity Law (China), *supra* note 26, art. 41; Personal Information Protection Law (China), *supra* note 28, arts. 13, 17.

[62] Personal Information Protection Law (China), *supra* note 28, arts. 17, 22–23, 30, 35, 39, 57.

disclosure, theft, tampering, and loss of personal information.[63] They are also prohibited from selling or unlawfully providing personal information to others, collecting or handling personal information that is excessive or unrelated to the services provided, stealing or otherwise unlawfully acquiring personal information, and disclosing or tampering with personal information.[64] Where businesses use personal information in automated decision-making, they must not engage in unreasonable differential treatment and, if using it to conduct information push delivery or commercial selling, they must also provide non-tailored options and the option to refuse.[65] Further, some digital platforms[66] that handle personal information are required to actively supervise the handling of personal information on their platforms.[67]

Third, the state's ability to access, control, and use personal information does not appear to be significantly constrained by the data governance laws. State authorities that collect or use personal information in carrying out their legally prescribed duties have limited obligations. They are required to ensure that their collection and use of personal information is within the scope of their duties and only to the extent necessary to carry out their duties,[68] to maintain the confidentiality of personal information they come across in carrying out their duties, to not disclose or unlawfully provide that information to third parties, and to provide individuals with certain information.[69] Beyond these specified obligations, it is unclear whether state authorities need to comply with the obligations that are required of other handlers of personal information; but, in any event, the Personal Information Protection Law expressly provides that there is no need to obtain consent to collect, handle, or use personal information where it is necessary to carry out statutory duties, responsibilities, and obligations.[70] Further, no consent is required in situations involving national security and defense, public security, public health and safety, significant public interests, criminal investigation and enforcement, emergencies, and news reporting, public opinion oversight, and similar activities in the public interest,[71] which are situations that are often within the scope of responsibilities for state authorities.

---

[63] Cybersecurity Law (China), *supra* note 26, arts. 21, 42; *id*. arts. 51, 57.

[64] *Id.* arts. 27, 41–42, 44; Personal Information Protection Law (China), *supra* note 28, arts. 5–6, 10, 25.

[65] Personal Information Protection Law (China), *supra* note 28, art. 24.

[66] Personal information handlers that provide digital platform services, have a large number of users, and adopt complex business models. *Id.* art. 58.

[67] *Id.*

[68] *Id.* art. 34.

[69] Cybersecurity Law (China), *supra* note 26, art. 45; *id*. art. 35.

[70] Personal Information Protection Law (China), *supra* note 28, art. 13.

[71] *Id.*; Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (Guojia Biaozhun GB/T 35273-2020) (信息安全技术个人信息安全规范 (国家标准GB/T 35273-2020)) [Information Security Technology—Personal Information Security Specification (National Standard GB/T 35273-

This analysis shows that national security, public security, public interest, development, commercial, and privacy concerns relating to data are all featured and balanced within the data regulatory legal framework. This is especially highlighted in how personal information is regulated under the data governance laws. Not only does the data governance regime respond to growing consumer demands for personal information rights and protections, but it does so in a manner that does not significantly constrain the state. The pursuit of these two seemingly contradictory aims is made possible because businesses bear most of the obligations and restrictions. Moreover, the data governance laws recognize that even personal information may be a public commodity with implications for national security, public security, and development, and it may be regulated as such.

These various concerns, goals, and interests are also reflected in the complicated administrative enforcement arrangements that underlie the data regulatory regime. Under the Cybersecurity Law, the Cyberspace Administration of China[72] (CAC) is responsible for planning, coordinating, supervising, and managing cybersecurity work and the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS) are responsible for cybersecurity protection, supervision, and management within the scope of their responsibilities.[73] The enforcement of the Data Security Law is led by the Central Leading Authority on National Security, and the CAC, MPS, Ministry for State Security (MSS), and regulatory departments in each region are responsible for the data collected and data security in their own region.[74] Similarly, the Personal Information Protection Law provides that the CAC is responsible for planning, coordinating, supervising, and managing the state's personal information protection work and formulating rules and standards to implement the law, whereas each government department is responsible for personal information protection, supervision, and management within their own scope of duties and responsibilities.[75]

These enforcement arrangements highlight the fact that the state's goals, concerns, and interests relating to data are not uniform. The mix of authorities involved in data governance is very broad, and none of them have, as their focus, data governance. For example, the CAC is responsible for cybersecurity, informatization, and online content governance, the MIIT is the sector regulator for the information technology and telecommunications in-

---

2020)] (promulgated by the State Admin. for Mkt. Reg, Mar. 7, 2020, effective Oct. 1, 2020) (China), ¶ 5.6.

[72] The Cyberspace Administration of China is also called the State Internet Information Office.

[73] Cybersecurity Law (China), *supra* note 26, art. 8.

[74] Data Security Law (China), *supra* note 27, arts. 5–6.

[75] Personal Information Protection Law (China), *supra* note 28, arts. 60–62.

dustries, the MSS is responsible for national (political and domestic) security and China's intelligence-related work, and the MPS is responsible for criminal enforcement and public security. Enforcement is dispersed horizontally (across ministries, departments, and party authorities with different functional areas) and vertically (across different levels of government and geographic regions), meaning that a multitude of central and local state authorities are involved in data governance. The different backgrounds and purviews of these authorities might mean that they have divergent views on and approaches to data and data governance and this can lead to inconsistencies, tensions, and even conflict within the state when it comes to data-related matters.

C. OTHER AVENUES OF STATE INFLUENCE AND CONTROL

The data governance laws provide the Chinese government with the basic legal means to directly regulate the data and data practices of internet and technology businesses. The state also has other formal and informal means to help it to control and influence the data-related activities of internet and technology businesses and obtain access to their data. In particular, growth and innovation in China's digital economy has been driven by private companies, and China's leading internet and technology companies are privately owned.[76] The Chinese Communist Party has made it very clear that it aims to strengthen its control and influence over private companies and entrepreneurs to support its political goals[77] and prevent the "disorderly expansion of capital."[78]

At the most basic level, compliance with laws and regulations is a condition of access to China's sizable market. While this is a standard requirement across all countries, it does mean that internet and technology companies, whether Chinese or non-Chinese, state-owned or privately-owned, must, *inter alia*, comply with strict censorship and information control requirements;[79]

---

[76] *See e.g.*, *Zhongguo Hulianwang Qiye Zonghe Shili Zhishu (2021) Zhengshi Fabu* (中国互联网企业综合实力指数 (2021) 正式发布) [Official Release of the 2021 Comprehensive Strength Index of Chinese Internet Companies], INTERNET SOC'Y OF CHINA (Nov. 26, 2021), www.isc.org.cn/article/10905751852283850 5.html. According to this list, the top 10 Chinese internet companies in 2021 are Alibaba, Tencent, Baidu, Jingdong, Meituan, ByteDance, Pinduoduo, NetEase, and Kuaishou; these are all private companies.

[77] Jiaqiang Xin Shidai Minying Jingji Tongzhan Gongzuo De Yijian (加强新时代民营经济统战工作的意见) [Opinions on Strengthening the United Front Work Relating to the Private Economy in the New Era] (promulgated by the Gen. Office Cent. Comm. Communist Party of China, Sept. 15, 2020) (China).

[78] *Xi Focus: Xi Chairs Leadership Meeting on Economic Work for 2021*, XINHUA (Dec. 11, 2020), www.xinhuanet.com/english/2020-12/11/c_139582746.htm.

[79] Jiang & Fu, *supra* note 16, at 386; RUAN, *supra* note 16, at 7; John Lee, *The Rise of China's Tech Sector: The Making of an Internet Empire*, THE INTERPRETER (May 4, 2017), www.lowyinstitute.org/the-interpreter/rise-china-s-tech-sector-making-internet-empire.

help China maintain national security;[80] and support, assist, and cooperate with national intelligence efforts.[81] Companies that refuse to comply with these requirements—which could relate to how they collect, share, and handle their data—are denied access to the Chinese market. For example, Google's refusal to comply with China's censorship requirements led to the removal of its search services from China in 2010,[82] whereas Apple complies with censorship demands and the requirement to host relevant data in mainland China.[83]

The state has policies and other supports to incentivize internet and technology companies to act to forward the state's interests in data. Internet and related technology sectors are earmarked as priority sectors for development in major development plans and policies that are adopted by the state. For example, the Chinese government has adopted a number of major policies—such as the "Internet Plus" Action Plan, Made in China 2025, and the National Informatization Development Strategy—to foster the development and growth of Chinese internet and information technology companies,[84] furthering its goal of becoming a world-leading internet industrial superpower with a number of globally competitive multinational internet and information technology companies by 2025.[85] The use and development of data feature in these major plans and policies. Companies that respond by directing and using their data to develop technologies that carry out the state's policies will benefit from favorable measures, such as access to funding, subsidies, and a more favorable regulatory environment generally.[86] Further, companies that are designated as "national champions" or part of the "national team" are afforded even more benefits and privileges, including financial and other support to

---

[80] Guojia Anquan Fa (国家安全法) [National Security Law] (promulgated by the Standing Comm. Nat'l People's Cong., July 1, 2015) (China) arts. 11, 77.

[81] Guojia Qingbao Fa (国家情报法) [National Intelligence Law] (promulgated by the Standing Comm. Nat'l People's Cong., June 27, 2017, effective June 28, 2017) (China), art. 7.

[82] Google started operations in China in 2006 and had provided a search engine with censored results, but in 2010 it stopped its censored search services in China and redirected users to its uncensored search engine in Hong Kong, which become inaccessible soon after. *See generally* Justine Lau, *A History of Google in China*, FIN. TIMES (July 9, 2010); Matt Sheehan, *How Google Took on China—and Lost*, MIT TECH. REV. (Dec. 19, 2018), www.technologyreview.com/2018/12/19/138307/how-google-took-on-china-and-lost.

[83] For example, Apple removed certain apps from its Chinese app store and stores the data and encryption keys of Chinese iCloud accounts in mainland China. *See, e.g.*, Stephen Nellis & Cate Cadell, *Apple Moves to Store iCloud Keys in China, Raising Human Rights Fears*, REUTERS (Feb. 24, 2018), www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060.

[84] *See, e.g.*, Xie Yu, *China Sets Up 100 Billion Yuan State Fund to Invest in the Internet*, S. CHINA MORNING POST (Jan. 22, 2017); Lee, *supra* note 79; Hao Chen & Meg Rithmire, *The Rise of the Investor State: State Capital in the Chinese Economy*, 55 STUD. IN COMP. INT'L DEV. 257, 261–62 (2020).

[85] Outline for the National Informatization Development Strategy, *supra* note 22.

[86] *See* Jiang & Fu, *supra* note 16, at 385–86; RUAN, *supra* note 16, at 7.

expand and compete internationally.[87] This designation provides these companies with privileged positions, including in relation to standard setting and protection from competition from state-owned enterprises.[88] These state policy measures therefore help to better align the commercial interests of internet and technology companies in data with those of the state's, and narrow the gap between them.[89]

The state also can influence and monitor the data and activities of internet and technology companies from within. While many Chinese internet and technology companies are privately owned, the state still has a presence within private companies. Nearly 68 percent of all Chinese private companies had established party committees by the end of 2016,[90] and that percentage is believed to be even higher at leading Chinese internet and technology companies, with reports that all of the top 100 internet companies in China have party committees.[91] It has also been reported that "Tencent, Alibaba and Baidu have all been forced to accept Party representation on their boards because of their sheer size."[92] The leaders of some of the largest Chinese internet and technology companies are members of political bodies such as the National People's Congress and the Chinese People's Political Consultative Conference.[93] There are also reports that the government has discussed taking, or has taken, small ownership interests in some large internet companies.[94] These

---

[87] *See, e.g.*, Lindsay Maizland & Andrew Chatzky, *Huawei: China's Controversial Tech Giant*, COUNCIL ON FOREIGN RELS. (Aug. 6, 2020), www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

[88] GREGORY C. ALLEN, UNDERSTANDING CHINA'S AI STRATEGY: CLUES TO CHINESE STRATEGIC THINKING ON ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY 21 (2019), www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

[89] Jiang & Fu, *supra* note 16, at 384–86.

[90] Zhang Lin, *Chinese Communist Party Needs to Curtail Its Presence in Private Businesses*, S. CHINA MORNING POST (Nov. 25, 2018).

[91] Liu Yun & Sun Zhongfa, *Woguo Hulianwang Qiye Yongdong "Dang Jianchao"* (我国互联网企业涌动"党建潮") [China's Internet Companies' Surging "Party Building Tide"], ZHONGGUO ZHUZHI RENSHI BAO (中国组织人事报) (Mar. 26, 2018), dangjian.people.com.cn/n1/2018/0326/c117092-29889441.html; *see also* Elliott Zaagman, *China: How Big Tech Is Learning to Love the Party*, THE INTERPRETER (Oct. 17, 2018), www.lowyinstitute.org/the-interpreter/china-how-big-tech-learning-love-party. Where there are three or more full CCP members within an organization, members are required to form a party committee. ZHONGGUO GONGCHANDANG ZHANGCHENG (中国共产党章程) [Constitution of the Communist Party of China] art. 30 (Oct. 24, 2017).

[92] Erica Pandey, *Caged Giants: Why China's Big Tech Can't Escape the Communist Party*, AXIOS (June 8, 2018), www.axios.com/china-big-tech-alibaba-tencent-communist-party-xi-jinping-c9de0516-1315-41e8-9daa-932c57f7faec.html.

[93] Kenji Kawase, *In China, Private Companies Walk a Fine Line*, NIKKEI ASIAN REV. (May 23, 2018), asia.nikkei.com/Spotlight/Cover-Story/In-China-private-companies-walk-a-fine-line2; Curtis J. Milhaupt & Wentong Zheng, *Beyond Ownership: State Capitalism and the Chinese Firm*, 103 GEO. L.J. 665, 684 (2015).

[94] Li Yuan, *Beijing Pushes for a Direct Hand in China's Big Tech Firms*, WALL ST. J. (Oct. 11, 2017); Juro Osawa & Shai Oster, *Beijing Tightens Grip on ByteDance by Quietly Taking*

developments point to the increasingly close political connections between private internet and technology companies and the state.

Even though the data governance laws and these other avenues help the state to regulate data from a variety of perspectives and means, the state's regulatory capabilities and powers are not complete nor incontrovertible. For instance, the Chinese state is not a homogeneous, uniform, or monolithic entity. The state bureaucracy is fragmented, and different state bodies, at both the central and local levels, may have varying and conflicting interests and political and economic incentives. This could result in centrally-set policies not being implemented at the local levels and in power struggles between different agencies and provinces, including over regulatory turf and data. Additionally, internet and technology companies do not always cooperate and comply with demands from state authorities, including those relating to access to data. Even though the room to challenge or resist the state's demands to access to data and cooperate on related matters is very limited, there have been instances where internet and technology companies have pushed back against the state's demand for data or cooperation, with varying degrees of success and consequences.[95]

D. Political Dynamics of Data Governance

The legal framework for data regulation, nestled within the other mechanisms of state influence and control, brings together myriad public and private stakeholders, interests, and objectives, not all of which are necessarily compatible with one another. It is unclear, for example, how conflicts, tensions, or inconsistencies within the data governance regime might be resolved, what types of trade-offs might be made, and how relationships and power dynamics between the different stakeholders might impact outcomes. This exercise of coordinating and balancing the interests and objectives of different stakeholders and their relationships occurs within the context of the state's influence and control over the digital economy and its participants.

To illustrate some of the political dynamics that might arise in data governance, this Part examines the Chinese government's enforcement campaign that targeted the personal information practices of mobile phone apps. In Jan-

---

Stake, China Board Seat, The Info. (Aug. 16, 2021), www.theinformation.com/articles/beijing-tightens-grip-on-bytedance-by-quietly-taking-stake-china-board-seat; *Fretting About Data Security, China's Government Expands Its Use of "Golden Shares*," Reuters (Dec. 16, 2021), www.reuters.com/markets/deals/exclusive-fretting-about-data-security-chinas-government-expands-its-use-golden-2021-12-15.

[95] *See, e.g.*, Chen Juan, *Didi Has Refused to Provide User Data to Authorities, Traffic Official Says*, Yicai Global (Aug. 29, 2018), www.yicaiglobal.com/news/didi-has-refused-to-provide-user-data-to-authorities-traffic-official-says; Yuan Yang & Nian Liu, *Alibaba and Tencent Refuse to Hand Loans Data to Beijing*, Fin. Times (Sept. 18, 2019); Sun Yu, *Jack Ma's Ant Defies Pressure from Beijing to Share More Customer Data*, Fin. Times (Mar. 2, 2021).

uary 2019, the CAC, MIIT, MPS, and State Administration for Market Regulation (SAMR) embarked on a joint one-year nationwide enforcement campaign targeting the illegal use and collection of personal information by apps ("App Personal Information Protection Campaign").[96] The primary purpose of this campaign was to secure and improve compliance with personal information protection obligations under the Cybersecurity Law.[97] The authorities identified, targeted, and rectified instances of non-compliance with the personal information protection obligations of network operators under the Cybersecurity Law.[98] In addition, the CAC and SAMR jointly established an app personal information security certification system, and the MIIT sought to improve the network data security capabilities of businesses operating in the telecommunications and internet sectors.[99] The four authorities also released two guidelines on how to identify the illegal collection and use of personal information by apps.[100] In July 2020, the CAC, MIIT, MPS, and SAMR announced another enforcement campaign to continue and build upon their joint work addressing the illegal collection and use of personal information by apps.[101]

---

[96] Guanyu Kaizhan App Weifa Weigui Shouji Shiyong Geren Xinxi Zhuanxiang Zhili De Gonggao (关于开展App违法违规收集使用个人信息专项治理的公告) [Announcement on the Launch of the Enforcement Campaign on the Illegal Collection and Use of Personal Information by Apps], Jan. 23, 2019 (Cyberspace Admin. of China, Ministry of Industr. and Info. Tech., Ministry of Pub. Sec., and State Admin. for Mkt. Reg.) (China).

[97] *Id.*

[98] Such conduct was (1) non-disclosure of rules governing the collection and use of personal information; (2) not clearly stating the purpose, mode, and scope of the collection and use of personal information; (3) collecting and using personal information without user consent; (4) collecting and using personal information that was unnecessary and unrelated to the provision of services; (5) providing personal information to others without consent; and (6) not providing functions that allowed for the deletion or correction of personal information: APP ZHUANXIANG ZHILI GONGZUO ZU (App专项治理工作组) [Personal Information Protection Taskforce on Apps], APP WEIFA WEIGUI SHOUJI SHIYONG GEREN XINXI ZHUANXIANG ZHILI BAOGAO (2019) (App违法违规收集使用个人信息专项治理报告(2019)) [App Breach of Laws and Regulations: Collecting and Using Personal Information Enforcement Campaign (2019)] 7 (2019), www.cac.gov.cn/2020-05/26/c_1592036763304447.htm.

[99] *Id.* at 5–6; Ken Dai & Jet Deng, 2019 China Data Protection & Cybersecurity Annual Report, DENTONS, Mar. 2020, at 15–20.

[100] App Weifa Weigui Shouji Shiyong Geren Xinxi Xingwei Rending Fangfa (App违法违规收集使用个人信息行为认定方法) [Method on How to Identify the Illegal Collection and Use of Personal Information by Apps] (promulgated by the Cyberspace Admin. of China, Ministry of Indust. and Info. Tech., Ministry of Pub. Sec., and State Admin. for Mkt. Reg., Nov. 28, 2019) (China); App Weifa Weigui Shouji Shiyong Geren Xinxi Zi Pinggu Zhinan (App违法违规收集使用个人信息自评估指南) [Guidelines on Self-Assessment for the Illegal Collection and Use of Personal Information by Apps] (promulgated by the Personal Info. Protection Taskforce on Apps, Mar. 1, 2019) (China).

[101] 2020 Nian App Weifa Weigui Shouji Shiyong Geren Xinxi Zhili Gongzuo Qidong Hui Zai Beijing Zhaokai (2020年App违法违规收集使用个人信息治理工作启动会在京召开) [App Illegal Collection and Use of Personal Information 2020 Governance Work Kick-Off Meeting Held in Beijing], CYBERSPACE ADMIN. OF CHINA (July 25, 2020), www.cac.gov.cn/2020-07/25/c_1597240741055830.htm.

A number of different interests, concerns, and goals are reflected and balanced in the App Personal Information Protection Campaign. The Chinese government recognizes that apps play an important role in furthering economic development and serving the public's needs and that personal information is a core, strategic, and valuable resource for businesses in the digital economy.[102] At the same time, the involvement of all three government authorities with enforcement responsibilities under the Cybersecurity Law—the CAC, MPS, and MIIT—reflects the cybersecurity, public security, and industrial policy lenses that they bring to the protection of personal information. Moreover, even though the SAMR does not have any responsibilities under the Cybersecurity Law, it is involved in the App Personal Information Protection Campaign because of its responsibilities enforcing the Consumer Rights Protection Law. This expressly highlights that protecting personal information is also a means of protecting the interests of consumers.

The fact that the Chinese government chose to use campaign-style enforcement to address the illegal collection and use of personal information by apps, rather than normal law enforcement processes and activities, provides some valuable insights into the political considerations and dynamics of personal information protection and data governance more broadly. First, it shows personal information protection has high-level political support and visibility. As Benjamin van Rooij observes, campaigns are called by political leaders, who do so in response to incidents that make it politically necessary for action to be taken.[103]

Second, the Chinese government has an evident interest in making sure that the public knows that it is taking personal information protection seriously and responding to the public's concerns.[104] There are growing concerns in China about the theft, leakage, and misuse of personal information, especially online, and increasing demands from the public for greater personal information protections.[105] Enforcement campaigns are very public in nature and often involve the public as well. As part of the 2019 App Personal Information Protection Campaign, members of the public were encouraged to, and did,

---

[102] Personal Information Protection Taskforce on Apps, *supra* note 98, at 1.

[103] Benjamin van Rooij, *The Campaign Enforcement Style: Chinese Practice in Context and Comparison*, *in* COMPARATIVE LAW AND REGULATION: UNDERSTANDING THE GLOBAL REGULATORY PROCESS 217, 220 (Francesca Bignami & David Zaring eds., 2016); *see also* Sarah Biddulph et al., *Rule of Law with Chinese Characteristics: The Role of Campaigns in Lawmaking*, 34 L. & POL'Y 373, 393, 395 (2012).

[104] van Rooij, *supra* note 103, at 230.

[105] *See, e.g.*, Yuan Yang, *China's Data Privacy Outcry Fuels Case for Tighter Rules*, FIN. TIMES (Oct. 1, 2018); Samm Sacks & Lorand Laskai, *China's Privacy Conundrum*, SLATE (Feb. 7, 2019), slate.com/technology/2019/02/china-consumer-data-protection-privacy-surveillance.html; *Public Pushback: In China, Consumers Are Becoming More Anxious About Data Privacy*, THE ECONOMIST (Jan. 25, 2018).

provide information, lodge complaints, and report violations by apps of personal information protections, and the results of the campaign (such as the number of apps reviewed, the number of instances of non-compliance found, the number of cases investigated, and total amount of fines imposed) were widely publicized through multiple media channels.[106] The campaign is an efficient and effective way for the Chinese government to clearly show the public that their demands and concerns about personal information were being responded to and addressed, which in turn helps to maintain the public's confidence in the state and ultimately enhance the legitimacy of its leadership. The campaign would have also helped the Chinese government to publicize its relatively new and developing policy and legal framework on personal information protection.

Third, the Chinese government faces some bureaucratic challenges in regulating and protecting personal information. As a variety of government authorities are involved in enforcing the Cybersecurity Law, this has led to turf wars and enforcement inconsistencies and inefficiencies.[107] The Chinese leadership has made several attempts over the past few years to centralize authority over cyberspace and internet activities and overcome these challenges.[108] Enforcement campaigns are used as a pragmatic tool to allow the central government to exercise short-term power over local governments, coordinate enforcement across multiple government authorities, and overcome resistance

---

[106] *See, e.g.*, Personal Information Protection Taskforce on Apps, *supra* note 98, at 3–6, 14–21; Shichang Jianguan Zongju Juxing "Baohu Xiaofei" Ji Daji Qinhai Xiaofeizhe Geren Xinxi Weifa Xingwei Zhuanxiang Zhifa Xingdong Fabuhui (市场监管总局举行"守护消费"暨打击侵害消费者个人信息违法行为专项执法行动发布会) [SAMR Holds Press Conference on its "Protecting Consumers" Enforcement Campaign Cracking Down on Infringements of Consumers' Personal Information], STATE COUNCIL INFO. OFFICE (Nov. 18, 2019), www.scio.gov.cn/xwfbh/gbwxwfbh/xwfbh/38173/Document/1668563/1668563.htm; Guojia Wangluo Anquan Tongbao Zhongxin (国家网络安全通报中心) [National Cybersecurity Notification Center], Gongan Jiguan Kaizhan App Weifa Caiji Geren Xinxi Jizhong Zhengzhi (公安机关开展APP违法采集个人信息集中整治) [Public Security Authorities Carry Out Centralised Rectification of the Illegal Collection of Personal Information by Apps], WEIXIN (Dec. 4. 2019), mp.weixin.qq.com/s/smT4RbHsA_x0vIZjEKV_yg.

[107] Wang Shenjun, Vice Chairman of the Standing Comm. Nat'l People's Cong., Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui Zhifa Jiancha Zu Guanyu Jiancha "Zhonghua Renmin Gongheguo Wangluo Anquan Fa," "Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui Guanyu Jiaqiang Wangluo Xinxi Baohu De Jueding" Shishi Qingkuang De Baogao (全国人民代表大会常务委员会执法检查组关于检查《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》实施情况的报告) [Report of the Law Enforcement Inspection Group of the Standing Committee of the National People's Congress on its Review of the Implementation of the Cybersecurity Law and the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection] (Dec. 24, 2017).

[108] Rogier Creemers et al., *China's Cyberspace Authorities Set to Gain Clout in Reorganization*, NEW AMERICA (Mar. 26, 2018), www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization.

from government authorities who may not otherwise support enforcement.[109] Additionally, the campaign would have helped the government to gather, coordinate, and use its limited enforcement resources in a targeted way to address personal information protection.

II. DATA UNDER CHINA'S COMPETITION LAWS

China's data governance regime has primarily focused on addressing the risks of data to national security, public security, and privacy, encouraging the use and development of data to further economic and development goals, and constraining the data-related activities of businesses while preserving the state's ability to access and use data. The impact of data and data practices on competition has not yet been expressly considered within the data governance framework.

China has two principal laws that deal with different aspects of competition. The Anti-Monopoly Law[110] (AML) prohibits horizontal and vertical monopoly agreements, abuses of market power, and anticompetitive mergers, and is in essence quite similar to the antitrust/competition laws of many other countries. It also prohibits anticompetitive abuses of administrative power. The Anti-Unfair Competition Law[111] (AUCL) covers a range of unfair competition practices, with a focus on the fairness of business transactions and business ethics.[112] Since March 2018, the SAMR has been responsible for enforcing both the AML and the AUCL, with the Price Supervision and Inspection and Anti-Unfair Competition Bureau being responsible for the AUCL and the State Anti-Monopoly Bureau responsible for the AML.[113] The AML and AUCL may also be enforced by private parties.

---

[109] van Rooij, *supra* note 103, at 220–21, 228; *see also* Biddulph et al., *supra* note 103, at 393, 395.

[110] Fanlongduan Fa (反垄断法) [Anti-Monopoly Law] (promulgated by the Standing Comm. Nat'l People's Cong., revised June 24, 2022, effective Aug. 1, 2022) (China).

[111] Fan Bu Zhendang Jingzheng Fa (反不正当竞争法) [Anti-Unfair Competition Law] (promulgated by the Standing Comm. Nat'l People's Cong., revised Nov. 4, 2017, effective Jan. 1, 2018) (China).

[112] The Anti-Unfair Competition Law (AUCL) applies to passing off, commercial bribery, misleading advertising, infringement of trade secrets, prize promotions, commercial slander and libel, and Internet-related conduct. *Id.* arts. 6–12; *see also* Meng Yanbei, *The Uneasy Relationship Between Antitrust and Anti-Unfair Competition Laws in China*, *in* WANG XIAOYE: THE PIONEER OF COMPETITION LAW IN CHINA 219 (Adrian Emch & Wendy Ng eds., 2019).

[113] Prior to March 2018, the Anti-Monopoly Law (AML) was enforced by three separate authorities (the Ministry of Commerce, the National Development and Reform Commission, and the State Administration for Industry and Commerce), and the AUCL was enforced by the State Administration for Industry and Commerce.

A. DATA UNDER THE ANTI-UNFAIR COMPETITION LAW

Where the competitive impacts of data have been examined under the AUCL, it has typically been in private litigation cases involving the appropriation and use of data by one business from another business's website or digital platform without authorization. This conduct has been examined under Article 2 of the AUCL, which is the catch-all provision that requires businesses to abide by the principles of voluntariness, equality, fairness, and trustworthiness, and to comply with laws and business ethics. In particular, courts have looked at the impact of the unauthorized appropriation and use of data on commercial interests and the compatibility of that conduct with notions of business ethics.[114] For example, the failure of a business to obtain the three necessary authorizations—from the user to the data controller, from the user to the business wanting to take and use that data, and from the data controller to that business—before taking user data from another business's website or digital platform for its own use has been regarded as being contrary to business ethics and therefore in breach of Article 2 of the AUCL.[115] Similarly, courts have found that the appropriation and use of data that harms or jeopardizes data security, infringes on data rights and interests (such as users' personal information protection and privacy rights), adversely affects the goods or services offered by a business, harms or undermines a business's competitive advantage or commercial benefits, or breaches relevant laws and regula-

---

[114] *See, e.g.*, Beijing Baidu Wangxun Keji Youxian Gongsi Yu Shanghai Hantao Xinxi Zixun Youxian Gongsi Bu Zhengdang Jingzheng Jiufen Minshi Panjueshu (北京百度网讯科技有限公司与上海汉涛信息咨询有限公司不正当竞争纠纷民事判决书) [Beijing Baidu Netcom Science Technology Co Ltd and Shanghai Hantao Information Consulting Co Ltd Unfair Competition Dispute Civil Judgment], (2016) Hu 73 Min Zhong 242 Hao ((2016) 沪73民终242号), Aug. 30, 2017 (Shanghai Intell. Prop. Ct. 2016) (China) [hereinafter *Baidu v. Hantao*]; Beijing Taoyou Tianxia Jishu Youxian Gongsi Deng Yu Beijing Weimeng Chuangke Wangluo Jishu Youxian Gongsi Bu Zhengdang Jingzheng Jiufen Ershen Minshi Panjue Shu (北京淘友天下技术有限公司等与北京微梦创科网络技术有限公司不正当竞争纠纷二审民事判决书) [Beijing Taoyou Tianxia Technology Co Ltd and Beijing Weimeng Chuangke Network Technology Co Ltd Unfair Competition Dispute Second Instance Civil Judgment], (2016) Jing 73 Min Zhong 588 Hao ((2016) 京73民终588号), Dec. 30, 2016 (Beijing Intell. Prop. Ct. 2016) (China) [hereinafter *Sina Weibo v. Maimai*]; Shenzhen Shi Tengxun Jisuanji Xitong Youxian Gongsi Yu Beijing Weibo Shijie Keji Youxian Gongsi Bu Zhengdang Jingzheng Jiufen Minshi Caiding Shu (深圳市腾讯计算机系统有限公司与北京微播视界科技有限公司不正当竞争纠纷民事裁定书) [Shenzhen Tencent Computer System Co Ltd and Beijing Weibo Vision Technology Co Ltd Unfair Competition Dispute Civil Judgment], (2019) Jin 0116 Min Chu 2091 Hao ((2019) 津0116民初2091号), Mar. 18, 2019 (Tianjin Binhai New District People's Ct. 2019) (China) [hereinafter *Tencent v. Douyin*]; Beijing Weimeng Chuangke Wangluo Jishu Youxian Gongsi Yu Shanghai Fuyu Wenhua Chuanbo Gufen Youxian Gongsi Bu Zhengdang Jingzheng Jiufen Minshi Panjue Shu (北京微梦创科网络技术有限公司与上海复娱文化传播股份有限公司不正当竞争纠纷民事判决书) [Beijing Weimeng Chuangke Network Technology Co Ltd and Shanghai Foyo Culture & Entertainment Co Ltd Unfair Competition Dispute Civil Judgment], (2017) Jing 0108 Min Chu 24510 Hao ((2017) 京0108民初24510号), June 30, 2019 (Beijing Haidian District People's Ct. 2019) (China).

[115] *Sina Weibo v. Maimai*, *supra* note 114; *Tencent v. Douyin*, *supra* note 114.

tions (such as the Cybersecurity Law) to be unfair competition conduct due to the impact on business interests and incompatibility with ethical business behavior.[116]

In these cases, the courts have distinguished between the two different types of data—the data resource as a whole and the data relating to specific individuals—that are on digital platforms and considered their implications for unfair competition. While the overall data resource is owned by the digital platform because it is the product of its investment of resources, the individual-specific data belongs to those individuals who created the data; as such, the digital platform only has a right to use that data in accordance with its user agreement and the principles of consent, lawfulness, and necessity. Courts have said that, even though the unauthorized appropriation and use of user-related data by another business interferes with the data rights of users, such conduct can nonetheless breach the AUCL because it harms the competitive advantage and commercial benefits that the digital platform derives from its ownership of the overall data resource.[117]

B. DATA UNDER THE ANTI-MONOPOLY LAW

Data and related issues have been considered for their impact on competition under the AML across abuse of dominance, merger, and monopoly agreements, to varying degrees. Until relatively recently, data had not really been considered in abuse of dominance cases. The Supreme People's Court in *Qihoo 360 v. Tencent* had, when evaluating whether Tencent had engaged in tying conduct in breach of Article 17(4) of the AML, briefly considered data security as an attribute of product and service quality and as a valid justification for having engaged in conduct.[118]

---

[116] *See, e.g.*, *Tencent v. Douyin*, *supra* note 114; *Sina Weibo v. Maimai*, *supra* note 114; *Baidu v. Hantao*, *supra* note 114; Taobao (Zhongguo) Ruanjian Youxian Gongsi Yu Anhui Meijing Xinxi Keji Youxian Gongsi Bu Zhengdang Jingzheng Jiufen Minshi Caiding Shu (淘宝(中国)软件有限公司与安徽美景信息科技有限公司不正当竞争纠纷民事裁定书) [Taobao (China) Software Co Ltd and Anhui Meijing Information Technology Co Ltd Unfair Competition Dispute Civil Judgment], (2017) Zhe 8601 Min Chu 4034 Hao ((2017) 浙8601民初4034号), Aug. 16, 2018 (Hangzhou Railway Transportation Ct. 2019) (China).

[117] Shenzhen Shi Tengxun Jisuanji Xitong Youxian Gongsi Yu Zhejiang Soudao Wangluo Jishu Youxian Gongsi Bu Zhengdang Jingzheng Jiufen Minshi Caiding Shu (深圳市腾讯计算机系统有限公司与浙江搜道网络技术有限公司不正当竞争纠纷民事裁定书) [Shenzhen Tencent Computer System Co Ltd and Zhejiang Soudao Network Technology Co Ltd Unfair Competition Dispute Civil Judgment], (2019) Zhe 8601 Min Chu 1987 Hao ((2019) 浙8601民初1987号), June 2, 2020 (Hangzhou Railway Transportation Ct. 2019) (China); *see also Sina Weibo v. Maimai*, *supra* note 114.

[118] Qihu Gongsi Yu Tengxun Gongsi Longduan Jiufen Shangsu An Panjue Shu (奇虎公司与腾讯公司垄断纠纷上诉案判决书) [Judgment on the Appeal of the Monopoly Dispute Between Qihoo and Tencent], (2013) Min San Zhong Zi 4 Hao ((2013) 民三终字第4号), Oct. 8, 2014 (Sup. People's Ct. 2013) (China) [hereinafter *Qihoo 360 v. Tencent*]. The Supreme People's Court briefly noted that it made sense to install the QQ security software with the QQ

This changed with the SAMR's recent abuse of dominance cases involving digital platforms, namely Alibaba[119] and Meituan.[120] In these cases, although the conduct under investigation was not centered upon data, data were relevant factors in defining the relevant markets, determining dominance, and identifying the abuse of dominance conduct, and were aspects of the commitments that Alibaba and Meituan were required to implement. The ability of online platforms to analyze and use data to enhance their services was a key reason why the SAMR decided that the online and offline services were not in the same relevant market.[121] In determining that Alibaba and Meituan had dominant positions in their respective markets,[122] the SAMR concluded that their accumulation of significant volumes of data and ability to analyze, process, and use that data were technological and competitive advantages that consolidated and strengthened their market power.[123] The SAMR also considered that data, data systems, and algorithms were key components of platform infrastructure that made market entry difficult, and recognized that data was a switching cost for customers, as it was difficult for businesses to migrate the data accumulated on a platform to competing platforms. When identifying the abuse of dominance conduct, the SAMR found that Alibaba and Meituan had, *inter alia*, used data, algorithms, and other technological means to monitor and ensure their customers' compliance with platform rules, which prevented

---

instant messaging software because it would help to ensure account security, therefore increasing the value and performance of the instant messaging software and enhancing efficiency.

[119] Xingzheng Chufa Jueding Shu (行政处罚决定书) [Administrative Penalty Decision], Guoshi Jianchu (2021) 28 Hao (国市监处 (2021) 28号, Apr. 10, 2021 (State Admin. for Mkt. Reg. 2021) (China) [hereinafter *SAMR Alibaba Abuse of Dominance Decision*].

[120] Xingzheng Chufa Jueding Shu (行政处罚决定书) [Administrative Penalty Decision], Guoshi Jianchu Fa (2021) 74 Hao (国市监处罚 (2021) 74号), Oct. 8, 2021 (State Admin. for Mkt. Reg. 2021) (China) [hereinafter *SAMR Meituan Abuse of Dominance Decision*].

[121] *Id*; *SAMR Alibaba Abuse of Dominance Decision*, *supra* note 119. The SAMR found that the online platform service and offline service were not in the same market in part due to the ability of the online platform to use big data, algorithms, and other technology to analyze and understand their customers and therefore the online platform was able to provide more tailored information and product and service offerings to customers and better match supply with demand, whereas offline services are less able to do so due to various limitations and difficulties.

[122] The SAMR concluded that Alibaba had a dominant market position in the online retail platform services market in China and that Meituan had a dominant market position in the online takeaway food and beverage services market in China. *SAMR Alibaba Abuse of Dominance Decision*, *supra* note 119; *SAMR Meituan Abuse of Dominance Decision*, *supra* note 120.

[123] This is consistent with the SAMR Shanghai authority's December 2020 decision in relation to its investigation of Sherpa's abuse of dominance conduct. In that decision, the Shanghai authority determined that Sherpa's had a dominant position in the English-language online food delivery platform service in Shanghai because, *inter alia*, Sherpa's had accumulated significant data resources and had a large advantage over its competitors in terms of its ability to obtain, analyze, and use that data, which enhanced its competitive advantage: Xingzheng Chufa Jueding Shu (行政处罚决定书) [Administrative Penalty Decision], Hu Shi Jian Fanlong Chu (2020) 06201901001 Hao (沪市监反垄处 (2020) 06201901001号 (2020) 行政指导书), Dec. 25, 2020 (Shanghai Admin. for Mkt. Reg. 2020) (China).

customers from dealing with competitors.[124] Additionally, some of the commitments that Alibaba and Meituan were requested to implement related to their data and data practices.[125] Both companies were asked not to use data, algorithms, platform rules, and other technological means to implement monopoly agreements, engage in abuse of dominance conduct, and exclude or restrict competition, and to protect personal information and privacy, with Meituan specifically requested not to collect personal information illegally.[126] Alibaba was also asked to use its data resources in a fair and impartial manner and to enhance the openness of the data interface on its platform.[127] The first private litigation case concerning data under the AML was also taken recently, when Sina Weibo, one of the largest social media platforms in China, was sued for allegedly abusing its dominance by refusing to grant access to its data.[128]

Data issues have also been raised in some mergers and monopoly agreement cases, and most of these cases did not involve companies operating in digital markets. One of the competition concerns raised in merger review has been that the acquirer would, by reason of the merger, gain access to certain data and have the ability and incentive to use that data to adversely affect competition. To resolve such concerns, merging parties have given commitments to provide access to data, to restrict or prevent the exchange and sharing of data, and to adopt measures to protect data.[129] The exchange of data

---

[124] *SAMR Alibaba Abuse of Dominance Decision*, *supra* note 119.

[125] Xingzheng Zhidao Shu (行政指导书) [Administrative Guidance], Guo Shi Jian Xingzhi Fanlong (2021) 1 Hao (国市监行指反垄 (2021) 1号, Apr. 6, 2021 (State Admin. for Mkt. Reg. 2021) (China) [hereinafter *SAMR Alibaba Abuse of Dominance Guidance*]; Xingzheng Zhidao Shu (行政指导书) [Administrative Guidance], Guo Shi Jian Xingzhi (2021) 1 Hao (国市监行指 (2021) 2号), Oct. 8, 2021 (State Admin. for Mkt. Reg. 2021) (China) [hereinafter *SAMR Meituan Abuse of Dominance Guidance*].

[126] *SAMR Alibaba Abuse of Dominance Guidance*, *supra* note 125; *SAMR Meituan Abuse of Dominance Guidance*, *supra* note 125.

[127] *SAMR Alibaba Abuse of Dominance Guidance*, *supra* note 125.

[128] Xinmei Shen, *Weibo Sued for Monopolistic Practices Limiting Access to Its Data as China's Antitrust Crackdown Invites New Challenges*, S. CHINA MORNING POST (Nov. 10, 2021).

[129] *See, e.g.*, Guanyu Fu Tiaojian Pizhun Meiguo Tongyong Qiche Gongsi Shougou Deerfu Gongsi Fanlongduan Shencha Jueding De Gonggao (关于附条件批准美国通用汽车公司收购德尔福公司反垄断审查决定的公告) [Announcement of the Anti-Monopoly Review Decision to Conditionally Approve General Motor Corporation's Acquisition of Delphi Corporation], Gonggao 2009 Nian Di 76 Hao (公告2009年第76号) [Order No. 76 of 2009], Sept. 28, 2009 (Ministry of Com. 2009) (China); Guanyu Fujia Xianzhixing Tiaojian Pizhun Anmou Gongsi, Jiede Gongsi He Jinyatuo Gongsi Zujian Heying Qiye Jingyingzhe Jizhong Fanlongduan Shencha Jueding de Gonggao (关于附加限制性条件批准安谋公司、捷德公司和金雅拓公司组建合营企业经营者集中反垄断审查决定的公告) [Announcement of the Concentration of Business Operators Anti-Monopoly Review Decision to Attach Restrictive Conditions to the Approval of the Establishment of a Joint Venture between ARM, Giesecke & Devrient, and Gemalto], Gonggao 2012 Nian Di 87 Hao (公告2012年第87号) [Order No. 87 of 2012], Dec. 6, 2012 (Ministry of Com. 2012) (China); Guanyu Fujia Xianzhixing Tiaojian Pizhun Jiayang Gongsi Yu Sasi Kache Wen Jiafei Gongsi Hebing An Jingyingzhe Jizhong Fanlongduan Shencha

between parties, whether written or oral, through formal or informal or direct and indirect means, has supported findings that monopoly agreements have been reached or implemented.

C. UPDATING CHINA'S COMPETITION LAWS FOR THE DIGITAL ECONOMY

Until recently, data were not specifically referenced or addressed in China's competition statutes and regulations. The relevance and impact of data to competition are being recognized, to an extent, in the recent adjustments made to the competition law framework by China's lawmakers and the SAMR to better deal with some of the competition issues arising in the digital economy.

The AML was amended in June 2022 to, *inter alia*, strengthen the regulation and supervision of digital platforms whilst supporting their innovation and development.[130] The AML now sets out the general principle that businesses must not use data, algorithms, technology, capital advantages, and platform rules to engage in monopoly conduct that is prohibited by the AML, and it further specifies that businesses with dominant market positions are prohibited from using data, algorithms, technology, capital advantages, and platform rules to engage in abuse of dominance conduct.[131] The SAMR's approach to regulating digital platforms under the AML, as explained in its Anti-Monopoly Guidelines on the Platform Economy[132] that were adopted in February 2021, also expressly recognizes the relevance of data to abuse of dominance conduct, mergers, and monopoly agreements.

In determining whether a platform has a position of market dominance, the SAMR will consider the platform's ability to access, control, and process data as part of its technological circumstances, and it views data acquisition as a

---

Jueding de Gonggao (关于附加限制性条件批准加阳公司与萨斯喀彻温钾肥公司合并案经营者集中反垄断审查决定的公告) [Announcement of the Concentration of Business Operators Anti-Monopoly Review Decision to Attach Restrictive Conditions to the Approval of the Merger between Agrium Corporation and Potash Corporation of Saskatchewan], Gonggao 2017 Nian Di 75 Hao (公告2017年第75号) [Order No. 75 of 2017], Nov. 6, 2017 (Ministry of Com. 2017) (China); Shichang Jianguan Zongju Guanyu Fujia Xianzhixing Tiaojian Pizhun Yingweida Gongsi Shougou Mailuosi Keji Youxian Gongsi Guquan An Fanlongduan Shencha Jueding De Gonggao (市场监管总局关于附加限制性条件批准英伟达公司收购迈络思科技有限公司股权案反垄断审查决定的公告) [Announcement of the State Administration for Market Regulation Anti-Monopoly Review Decision to Attach Restrictive Conditions to the Approval of NVIDIA Corporation's Acquisition of Equity in Mellanox Technologies], Apr. 16, 2020 (State Admin. for Mkt. Reg. 2020) (China).

[130] Zhang Gong, Director, State Admin. for Mkt. Reg., Guanyu "Zhonghua Renmin Gongheguo Fanlongduan Fa (Xiugai Caoan)" De Shuoming (关于《中华人民共和国反垄断法(修正草案)》的说明) [An Explanation of the Anti-Monopoly Law of the People's Republic of China (Draft Amendment)] (Oct. 19, 2021).

[131] Anti-Monopoly Law (China), *supra* note 110, arts. 9, 22.

[132] Guanyu Pingtai Jingji Lingyu De Fanlongduan Zhinan (关于平台经济领域的反垄断指南) [Anti-Monopoly Guidelines on the Platform Economy] (promulgated by the State Council Anti-Monopoly Comm'n, Feb. 7, 2021) (China).

barrier to entry.[133] Similarly, the possession of data by a platform is a factor that the SAMR takes into account when determining whether a platform constitutes an essential facility.[134] The Guidelines also provide that a platform that compulsorily collects non-essential user information[135] or uses big data and algorithms to engage in differential treatment[136] might have abused its dominance, though the SAMR also recognizes that protecting data and transaction security may be a legitimate reason for engaging in the conduct.[137]

Data are also relevant to competition assessment and remedies in merger review. When the SAMR assesses the impact of a proposed merger on competition, it will consider the business's ability to access, control, and process data and to control data interfaces, regard data as a barrier to entry, and recognize that harm to the interests of consumers can result if the proposed merger provides the business with the ability and incentive to use consumer data inappropriately.[138] The merger conditions that the SAMR might impose can include requiring the merging parties to divest or provide access to their data.[139] The Guidelines also recognize the role that data can play in helping parties to reach and implement monopoly agreements, impose unreasonable trading conditions, and coordinate conduct in breach of the AML.[140]

In relation to the AUCL, when the AUCL was amended in 2017, an article was added to capture some common types of unfair competition practices that had emerged in the provision of goods and services online.[141] The SAMR is also, at the time of writing this article, planning to adopt regulations that specifically address unfair competition conduct in the internet sector under the AUCL.[142] In particular, there are some specific references to data-related issues in the August 2021 draft of these proposed unfair competition regula-

---

[133] *Id.* art. 11.

[134] *Id.* art. 14.

[135] *Id.* art. 16.

[136] *Id.* art. 17.

[137] *Id.* arts. 14–15.

[138] *Id.* art. 20.

[139] *Id.* art. 21.

[140] *Id.* 5–8, 15.

[141] Under Article 12 of the Anti-Unfair Competition Law, businesses must not: (1) insert a URL link or force a URL redirection in an online product or service lawfully provided by another business without their consent; (2) mislead, deceive, or force users to change, shut down or uninstall an online product or service lawfully provided by another business; (3) maliciously cause incompatibility with an online product or service lawfully provided by another business; and (4) engage in other conduct that hinders or destroys the normal operation of an online product or service lawfully provided by another business: Anti-Unfair Competition Law (China), *supra* note 111, art. 12.

[142] Jinzhi Wangluo Bu Zhengdang Jingzheng Xingwei Guiding (Gongkai Zhengqiu Yijian Gao) (禁止网络不正当竞争行为规定 (公开征求意见稿)) [Provisions on Prohibiting Internet-Related Unfair Competition Conduct (Draft for Public Comment)] (released by the State Admin. for Mkt. Reg., Aug. 17, 2021) (China).

tions. Businesses will be prohibited from using data, algorithms, and other technological means to hijack traffic or influence users' choices and as such hinder or destroy the normal operation of online goods or services lawfully provided by other businesses; illegally obtaining or using the data of other businesses; impairing the data security of other businesses' users; and using data, algorithms, and other technological means to gather and analyze information about their counterparties to implement discriminatory trading conditions.[143]

III. THE RELATIONSHIP BETWEEN COMPETITION LAW AND DATA REGULATION AND THE IMPLICATIONS FOR COMPETITION LAW ENFORCEMENT

Even though the data governance laws are the principal laws that directly regulate data in China, other laws can also regulate data. For example, as discussed in Part II above, China's competition laws are not only being applied to examine the impact of data and data practices on competition, they are also being updated to expressly incorporate some data-related issues. The data governance laws are still quite new, especially as the Data Security Law and Personal Information Protection Law were enacted and came into effect in 2021. As the data governance legal framework becomes increasingly detailed and comprehensive, its regulators become more accustomed and empowered to enforce these laws, and the number of cases taken under them grow, data regulation will likely come up against and interact more frequently with, *inter alia*, the competition laws. This raises questions about the relationship of data governance with other spheres of regulation. For example, where data and data practices fall within the scope of the data governance laws and competition laws, will both laws be enforced, or will one set of laws or regulator take priority over others? If there is tension or inconsistency between the competition laws and data governance laws, how might that be resolved? Will the application of and outcomes under the competition laws be influenced by the data governance regime, and vice versa?

This Part explores the relationship between competition law and data regulation and how it shapes the use of competition law to regulate data in China.[144] It does so by considering two key questions. First, whether there are situations where there may be greater scope and relevance for China's compe-

---

[143] *Id.* arts. 13, 20–21.

[144] The related issue of enforcing competition law at its intersection with consumer protection and privacy is being discussed and debated in other countries and at global levels. *See, e.g.*, ICN Steering Group, *ICN Steering Group Project—Competition Law Enforcement at the Intersection Between Competition, Consumer Protection, and Privacy* 1 (ICN Issues paper, 2021), www.internationalcompetitionnetwork.org/wp-content/uploads/2022/02/Intersection-Project-Issues-identification-paper.pdf.

tition laws to be applied to address data-related issues, be that alongside or to the exclusion of the data governance laws. Second, whether the enforcement of and outcomes under competition law might be influenced by data governance principles and outcomes.

The exploration of these two questions will engage with the various consumer, commercial, and state interests, concerns, and goals that arise at the interface of data regulation and competition. They are the threads that can span and link the two spheres of regulation. As with data regulation, the state coordinates and mediates a variety of interests and goals through competition law and is the ultimate arbiter of which goals and interests should be pursued, and how.[145] Preventing and prohibiting monopolistic and unfair competition conduct; protecting fair competition and the interests of consumers, businesses, and the public; improving economic efficiency; and promoting the healthy development of the socialist market economy are the express objectives of the AML and AUCL,[146] and monopolies and unfair and disorderly competition are viewed as harmful to markets, consumers, and economic development more generally.[147] At the same time, competition law is regarded and used as a tool of market supervision and regulation and as an economic policy that helps the state to manage and coordinate the relationship between the state and the market.[148] Understanding how concerns, objectives, and interests are coordinated, balanced, and prioritized within and across the two regulatory areas can provide valuable insights into how the state will approach and

---

[145] WENDY NG, THE POLITICAL ECONOMY OF COMPETITION LAW IN CHINA 259–60 (2018) [hereinafter NG, POLITICAL ECONOMY]; *see also* Wendy Ng, *State Interest and the State-Centered Approach to Competition Law in China*, 65 ANTITRUST BULL. 297, 310 (2020) [hereinafter Ng, *State Interest*].

[146] Anti-Monopoly Law (China), *supra* note 110, art. 1; Anti-Unfair Competition Law (China), *supra* note 111, art. 1.

[147] *See, e.g.*, Outline of the 14th Five-Year Plan, *supra* note 17, ch. 20 art. 3.

[148] Wendy Ng, *Changing Global Dynamics and International Competition Law: Considering China's Potential Impact*, 30 EUR. J. INT'L L. 1409, 1423–26 (2020); Zhang Mao, Director of the State Admin. for Mkt. Reg., Guanyu "Zhonghua Renmin Gongheguo Fan Bu Zhengdang Jingzheng Fa (Xiuding Caoan) De Shuoming (关于《中华人民共和国反不正当竞争法（修订草案）》的说明) [An Explanation of the "Anti-Unfair Competition Law (Revised Draft)"], 26th Meeting of the Standing Comm. of the Twelfth Nat'l People's Cong., Feb. 22, 2017). *See, also, e.g., Shichang Jianguan Zongju Chuanda Xuexi Xi Jinping Zong Shuji Zhongyao Jianghua Jingshen He Quanguo Lianghui Jingshen* (市场监管总局传达学习习近平总书记重要讲话精神和全国两会精神) [SAMR Conveys and Studies the Spirit of General Secretary Xi Jinping's Important Speech and the Two Sessions], PRICE SUPERVISION AND INSPECTION AND ANTI-UNFAIR COMPETITION BUREAU OF THE STATE ADMIN. FOR MKT. REG. (Aug. 10, 2020), www.samr.gov.cn/jjj/sjdt/tpxw/202008/t20200810_320637.html; Xi Jinping: Guanyu "Zhonggong Zhongyang Guanyu Zhiding Guomin Jingji He Shehui Fazhan Di Shisi Ge Wunian Guihua He 2035 Yuanjing Mubiao De Jianyi" De Shuoming (习近平: 关于《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》的说明) [Xi Jinping: Explaining the "Proposals of the Central Committee of the Communist Party of China on Formulating the Fourteenth Five-Year Plan for National Economic and Social Development and Long-term Goals for 2035"] (Nov. 3, 2020), cpc.people.com.cn/n1/2020/1104/c64094-31917783.html.

manage the issues that arise at the intersection of competition law and data regulation. It also places the spotlight squarely on the stakeholders, political economy, and wider political and social considerations that will likely shape how and which concerns, objectives, and interests will be addressed and pursued.

This approach is also consistent with China's broader attitude towards how data should be regulated. Not all data attract the same level and type of regulatory attention in China. The characterization of data as, for example, economic, personal, or state assets or as potential risks to national security or the public interest, will affect whether and how that data are regulated. As discussed in Part I, under the data governance laws, data are categorized based on their importance to economic and social development and their risk to national security, the public interest, and the rights of individuals and organizations. Further, data relating to national security, the lifeline of the national economy, important aspects of people's livelihoods, and major public interests are regarded as the state's core data. As such, engaging with the objectives, concerns, and interests of consumers, businesses, and the state implicated by data can help to determine how that data might be categorized, which in turn directly affects how they are regulated and managed. Some types of data are subject to stricter protections, oversight, and regulation than others, and different legal and policy bases—which could include the competition laws—may be used to carry out that regulation.

A. SCOPE FOR COMPETITION LAW TO REGULATE DATA AT THE INTERSECTION

Like other countries, matters relating to national and public security are politically sensitive and priorities for China. Even where there may be valid competition concerns about the way that data are collected, used, or shared, if that data or conduct relate more directly to national and public security concerns, it stands to reason that these national and public security concerns will be prioritized over the competition concerns and the data will be classified to reflect those concerns and regulated accordingly. The Cybersecurity Law and Data Security Law expressly deal with the national and public security implications of data and provide the state with the regulatory tools to deal with them directly and to achieve the desired outcome, whereas the competition laws do not, at least not directly. As such, where data and conduct implicate national and public security concerns and interests, the data governance laws will likely take precedence over (perhaps even to the exclusion of) the competition laws to directly regulate and address data-related concerns.

The space for China's competition laws to play a more prominent and meaningful role in regulating data may be greater where the competition concerns coincide with industrial policy, economic and social development, and

privacy issues. It is not unusual to see Chinese competition authorities apply the competition laws in a manner that addresses these very issues alongside conventional competition goals and concerns, such as economic efficiency, consumer welfare, and protecting competition. Many past cases have involved conduct and companies in sectors that are important to industrial policy or that relate to the supply of essential goods and services to the public, and compliance with laws and regulations, especially sector regulations, has also been considered as part of competition law analysis.[149] Further, as discussed in Part II, data protection has been a relevant factor in some of the Chinese courts' and competition authorities' decision-making under the competition laws. This enforcement experience suggests that, where this mix of interests, concerns, and objectives are involved, competition law may be a feasible avenue through which they are pursued, irrespective of whether the data governance laws are applied.

The weighing of interests, concerns, and goals relating to data and whether competition law will be used to regulate that data in those circumstances will also be shaped by the relationships between the SAMR and the array of state bodies with power to enforce the data governance laws. With multiple regulators, there may be bureaucratic turf wars and conflicting interests and goals. The relationships and interactions that the SAMR has with the state authorities involved in data regulation—predominantly the CAC, MIIT, MPS, and MSS—will be shaped in part by their relative political power and importance, as well as the political sensitivity of the concerns raised by the data and conduct involved and the public signals that the state wishes to send to external parties. The CAC is a relatively young regulator, established in 2014 initially to regulate online content, and it is both a government body and a party entity directly under the CCP Central Committee. Even though the CAC has often faced political and bureaucratic resistance and challenge from other state authorities that are unwilling to relinquish their regulatory turf,[150] over the past couple of years it has been gaining more political power as its regulatory scope has expanded, and it has taken more high-profile actions. For the MSS, MPS, and MIIT, their legacies and the broad and political nature of their remits mean that they are among the most politically powerful state bodies in China. To further their own interests, these other regulators could take their own enforcement actions under the data governance laws and seek to oppose, intervene in, or influence competition law actions taken by the SAMR that overlap with their own.

---

[149] *See, e.g.*, NG, POLITICAL ECONOMY, *supra* note 145, at 259–77; Ng, *State Interest*, *supra* note 145, at 304, 308–09; Yaotian Chai, *The New Anti-Unfair Competition Law of the People's Republic of China 2018*, 13 J. INTELL. PROP. L. & PRAC. 998, 1004 (2018).

[150] Creemers et al., *supra* note 108.

It has not been unprecedented for other state authorities to intervene in competition law investigations and disputes. For example, when Tencent made its instant messaging software incompatible with Qihoo 360's antivirus and privacy protection software, within a few weeks the MIIT had publicly criticized the two companies' behavior and ordered them to issue public apologies and resume cooperation, which they did even as they proceeded with various competition law court proceedings.[151] And, it is believed that the MIIT's strong opposition to the competition regulator's abuse of dominance investigation into China Telecom and China Unicom led to the acceptance of commitments rather than the imposition of fines to address the competition concerns.[152]

Even though the SAMR is more powerful than its predecessors,[153] it is still a relatively new government authority, and it is figuring out its relationships with other state bodies and the boundaries of their respective regulatory turfs. Nonetheless, the authority of both the SAMR and competition law has been noticeably strengthened since the regulatory and enforcement campaign targeting internet and technology companies began in 2020.

The SAMR was one of the first regulators to take swift and clear action to respond to the suspension of the Ant Group's initial public offering in November 2020. Within a matter of days, the SAMR had released a draft of the AML guidelines that would apply to digital platforms,[154] jointly held an administrative guidance meeting with other regulators that was attended by 27 of China's major digital platforms,[155] and started two investigations into past

---

[151] Guanyu Piping Beijing Qihu Keji Youxian Gongsi He Shenzhen Tengxun Jisuanji Xitong Youxian Gongsi De Tongbao (关于批评北京奇虎科技有限公司和深圳市腾讯计算机系统有限公司的通报) [Notice Criticizing Beijing Qihoo Technology Co., Ltd. and Shenzhen Tencent Computer System Co., Ltd.] (promulgated by the Ministry of Indust. and Info. Tech., Nov. 20, 2010) (China).

[152] NG, POLITICAL ECONOMY, *supra* note 145, at 254–56.

[153] The SAMR was formed from the former State Administrative for Industry and Commerce (which was responsible for enforcing the AUCL and the non-price non-merger related aspects of the AML), the China Food and Drug Administration, and the General Administration of Quality Supervision, Inspection and Quarantine.

[154] Guanyu Pingtai Jingji Lingyu De Fanlongduan Zhinan (Zhengqiu Yijian Gao) (关于平台经济领域的反垄断指南(征求意见稿)) [Antitrust Guidelines on the Platform Economy (Consultation Draft)] (released by the State Admin. for Mkt. Reg., Nov. 10, 2020) (China). This draft was finalized and adopted by the Anti-Monopoly Commission in February 2021.

[155] Shichang Jianguan Zongju, Zhongyang Wangxinban, Shuiwu Zongju Lianhe Zhaokai Guifan Xianshang Jingji Zhixu Xingzheng Zhidao Hui, Yaoqiu Hulianwang Pingtai Qiye Jianchi Yifa Hegui Jingying, Qianghua Ziwo Yueshu Guanli, Gongtong Cujin Xianshang Jingji Jiankang Guifan Fazhan (市场监管总局, 中央网信办, 税务总局联合召开规范线上经济秩序行政指导会, 要求互联网平台企业坚持依法合规经营 强化自我约束管理 共同促进线上经济健康规范发展) [State Administration for Market Regulation, Cyberspace Administration of China, and State Administration of Taxation Hold an Administrative Guidance Meeting to Regulate the Order of the Digital Economy, Require Digital Platforms to Conduct their Operations According to Law, Strengthen Self-Management, and Jointly Promote the Healthy and Orderly Develop-

mergers undertaken by Alibaba and Tencent.[156] Then in December 2020, it launched a high-profile antitrust investigation into Alibaba, which was treated as a matter of national political sensitivity,[157] and announced the imposition of the highest fines possible on Alibaba and Tencent for not notifying their past mergers to the competition authority for anti-monopoly review.[158] These early and decisive actions would have helped the SAMR to signal and establish itself as a responsive and effective regulator to China's top leaders, other regulators and state authorities, businesses, and the public, and demonstrated to them the utility and strategic value of the AML as a regulatory instrument.

Since then, the SAMR has, predominantly through the use of its competition law powers, become one of the most visible and active regulators taking action against internet and technology companies. It has imposed a record-breaking fine of over RMB18.2 billion on Alibaba for abuse of market dominance,[159] fined Meituan for abuse of dominance,[160] reportedly began an antitrust investigation into Didi Chuxing,[161] prohibited the merger of two large Chinese video game live streaming digital platforms,[162] and continued to pun-

---

ment of the Digital Economy] (State Admin. for Mkt. Reg. Nov. 6, 2020), www.samr.gov.cn/xw/zj/202011/t20201106_323156.html.

[156] Xingzheng Chufa Jueding Shu (行政处罚决定书) [Administrative Penalty Decision], Guoshi Jianchu (2020) 26 Hao (国市监处 (2020) 26号), Dec. 14, 2020 (State Admin. for Mkt. Reg. 2021) (China) [hereinafter *Alibaba Investment/Yintai Commercial Failure to Notify Decision*); Xingzheng Chufa Jueding Shu (行政处罚决定书) [Administrative Penalty Decision], Guoshi Jianchu (2020) 27 Hao (国市监处 (2020) 27号), Dec. 14, 2020 (State Admin. for Mkt. Reg. 2021) (China) [hereinafter *China Literature/New Classics Media Failure to Notify Decision*].

[157] Yuan Yang, *Beijing Orders Chinese Media to Censor Coverage of Alibaba Probe*, FIN. TIMES (Jan. 7, 2021).

[158] *Alibaba Investment/Yintai Commercial Failure to Notify Decision*, *supra* note 156; *China Literature/New Classics Media Failure to Notify Decision*, *supra* note 156; *see also* Shichang Jianguan Zongju Fanlongduan Ju Zhuyao Fuzeren Jiu Alibaba Touzi Shougou Yintai Shangye, Tengxun Konggu Qiye Yuewen Shougou Xinli Chuanmei, Fengchao Wangluo Shougou Zhongyou Zhidi San Qi Wei Yifa Shenbao Anjian Chufa Qingkuang Da Jizhe Wen (市场监管总局反垄断局主要负责人就阿里巴巴投资收购银泰商业、腾讯控股企业阅文收购新丽传媒、丰巢网络收购中邮智递三起未依法申报案件处罚情况答记者问) [Head of SAMR Anti-Monopoly Bureau Answers Reporters' Questions on Sanctions for Three Cases of Failure to Notify Relating to Alibaba Investment's Acquisition of Yintai Commercial, Tencent Holdings' China Literature's Acquisition of New Classics Media, and Fengchao Network Technology's Acquisition of China Post Smart Delivery], STATE ADMIN. FOR MKT. REG. (Dec. 14, 2020), www.samr.gov.cn/xw/zj/202012/t20201214_324336.html.

[159] *SAMR Alibaba Abuse of Dominance Decision*, *supra* note 119. The RMB 18.228 billion fine imposed on Alibaba is nearly three times the previous largest fine of RMB 6.088 billion that was imposed on Qualcomm in 2015.

[160] *SAMR Meituan Abuse of Dominance Decision*, *supra* note 120.

[161] Julie Zhu & Pei Li, *China's IPO-bound Didi Probed for Antitrust Violations—Sources*, REUTERS (June 17, 2021), www.reuters.com/business/autos-transportation/exclusive-chinas-ipo-bound-didi-probed-antitrust-violations-sources-2021-06-17.

[162] Shichang Jianguan Zongju Guanyu Jinzhi Huya Gongsi Yu Douyu Guoji Konggu Youxian Gongsi Hebing An Fanlongduan Shencha Jueding De Gonggao (市场监管总局关于禁止虎牙公司与斗鱼国际控股有限公司合并案反垄断审查决定的公告) [Announcement of the State

ish a range of internet and technology companies for not having reported their past mergers for anti-monopoly review.[163]

The SAMR's efforts have been recognized and supported by the highest levels of China's government. China's leaders have made it clear that competition law plays an important role in the Chinese government's efforts to rein in internet and technology companies, and they have expressly called for the strengthening of competition law efforts and for regulators to crack down on monopolies, promote fair competition, and strengthen antitrust supervision.[164] With the amended AML, China's lawmakers have given the SAMR stronger and wider enforcement powers. For example, the SAMR now has the ability to initiate investigations into mergers that do not reach the notification thresholds but which nonetheless have or could have the effect of eliminating or restricting competition,[165] and the administrative penalties that it can impose for breaches of the AML have been significantly increased.[166] Institutional changes have also been made to bolster competition law enforcement. In November 2021, the bureau responsible for the AML at the SAMR was elevated to deputy-ministerial status and re-launched as the State Anti-Monopoly Bureau, with the appointment of the deputy minister of the SAMR as its leader and a planned significant increase in personnel.[167] These boosts to the SAMR's legal, institutional, and political powers will, together with the new competition law regulations targeting the digital economy, help it to more strongly assert its competition law mandate in the internet and technology sector, including to regulate data and deal with any jurisdictional overlaps and tussles with other regulators over data.

Administration for Market Regulation on the Anti-Monopoly Review Decision Prohibiting the Merger of Huya Inc and DouYu International Holdings Limited], July 10, 2021 (State Admin. for Mkt. Reg 2021) (China). This was also the first time that China's competition regular had blocked a domestic merger on anti-monopoly grounds.

[163] While the SAMR has fined a range of internet and technology companies for not notifying their mergers for anti-monopoly review, including Baidu, Didi Chuxing, Ele.me, Dianping, and Taobao, the substantial majority of these decisions involved mergers undertaken by Alibaba and Tencent. Further, over 80% of the decisions made by the SAMR in 2021 relating to companies not notifying their mergers for anti-monopoly review involved internet and technology companies.

[164] *See, e.g.*, *Xi Focus: Xi Chairs Leadership Meeting on Economic Work for 2021, supra* note 78; Xi Jinping: Tuidong Pingtai Jingji Guifan Jiankang Chixu Fazhan (习近平: 推动平台经济规范健康持续发展) [Xi Jinping: Promoting the Healthy and Sustainable Development of the Platform Economy], YINGSHI (央视) [China Central Television] (Mar. 15, 2021), finance.sina.com.cn/china/2021-03-15/doc-ikknscsi5370359.shtml.

[165] Anti-Monopoly Law (China), *supra* note 110, art. 26.

[166] *Id.* arts. 56, 58, 62, 63.

[167] *China Appoints Chief of National Anti-Monopoly Bureau*, REUTERS (Nov. 15, 2021), www.reuters.com/business/china-appoints-chief-national-anti-monopoly-bureau-2021-11-15; *China Establishes Anti-Monopoly Bureau to Secure Fair Competition*, XINHUA (Nov. 19, 2021), www.news.cn/english/2021-11/19/c_1310320506.htm; Pei Li & Coco Liu, *China to Expand Anti-Monopoly Bureau as Crackdown Widens, Sources Say*, BLOOMBERG (Oct. 12, 2021).

That being said, the overriding state interest to regulate internet and technology companies more strictly has expanded the scope for *all* regulators to take action against internet and technology companies, especially digital platforms. Similar to other campaigns, this regulatory and enforcement campaign would have helped to overcome some of the political and bureaucratic constraints that may have protected internet and technology companies from regulatory action in the past, and it has incentivized and emboldened numerous state bodies to take regulatory action in the internet and technology sector.[168]

The CAC, like the SAMR, has been active and visible in the campaign, expanded its regulatory powers, and gained political clout as a result. For example, it launched cybersecurity reviews into several companies that had recently listed on U.S. stock exchanges, citing national security, data security, and personal information protection concerns.[169] In particular, its high-profile cybersecurity review of Didi Chuxing, the leading ride-hailing company in China, resulted in a fine of RMB 8.026 billion.[170] The CAC also ordered several hundred apps to rectify their illegal collection and use of personal infor-

---

[168] Zhang, *supra* note 6, at 38.

[169] Wangluo Anquan Shencha Bangongshi Guanyu Dui "Didi Chuxing" Qidong Wangluo Anquan Shencha De Gonggao (网络安全审查办公室关于对 "滴滴出行" 启动网络安全审查的公告) [Announcement of the Cybersecurity Review Office on Launching a Cybersecurity Review into Didi Chuxing], July 2, 2021 (Cyberspace Admin. of China) (China), www.cac.gov.cn/2021-07/02/c_1626811521011934.htm; Wangluo Anquan Shencha Bangongshi Guanyu Dui "Yun Manman", "Huoche Bang", "Boss Zhipin" Qidong Wangluo Anquan Shencha De Gonggao (网络安全审查办公室关于对 "运满满" "货车帮" "BOSS直聘" 启动网络安全审查的公告) [Announcement of the Cybersecurity Review Office on Launching a Cybersecurity Review into "Yun Manman", "Huoche Bang", and "Boss Zhipin"], July 5, 2021 (Cyberspace Admin. of China) (China), www.cac.gov.cn/2021-07/05/c_1627071328950274.htm.

[170] Guojia Hulianwang Xinxi Bangongshi Dui Didi Quanqiu Gufen Youxian Gongsi Yifa Zuochu Wangluo Anquan Shencha Xiangguan Xingzheng Chufa De Jueding (国家互联网信息办公室对滴滴全球股份有限公司依法作出网络安全审查相关行政处罚的决定) [Decision of the Cyberspace Administration of China on the Administrative Penalties Relating to the Cybersecurity Review of Didi Global Co. Ltd], July 21, 2022 (Cyberspace Admin. of China) (China), www.cac.gov.cn/2022-07/21/c_1660021534306352.htm.

mation[171] and fined some internet companies for publishing information in breach of, *inter alia*, the Cybersecurity Law.[172]

Additionally, while the SAMR and CAC have been the most prominent in this enforcement campaign, as in other campaigns, there has also been coordination and collaboration across regulators and other state authorities on some activities. For example, the MPS, MSS, Ministry of Natural Resources, Ministry of Transport, State Administration for Taxation, and the SAMR joined the CAC in carrying out the cybersecurity review into Didi Chuxing;[173] the SAMR, CAC, and State Administration for Taxation jointly ordered 34 of China's biggest digital platforms to self-examine and rectify their conduct;[174] and the CAC, MIIT, MPS, and SAMR embarked on a joint three-month cam-

---

[171] Guanyu Shuru Fa Deng 33 Kuan App Weifa Weigui Shouji Shiyong Geren Xinxi Qingkuang De Tongbao (关于输入法等33款App违法违规收集使用个人信息情况的通报) [Announcement on the Illegal Collection and Use of Personal Information by 33 Input Method and Other Apps], May 1, 2021 (Cyberspace Admin. of China) (China), www.cac.gov.cn/2021-04/30/c_1621370239178608.htm; Guanyu Tengxun Shouji Guanjia Deng 84 Kuan App Weifa Weigui Shouji Shiyong Geren Xinxi Qingkuang De Tongbao (关于腾讯手机管家等84款App违法违规收集使用个人信息情况的通报) [Announcement on the Illegal Collection and Use of Personal Information by 84 Apps Including Tencent Mobile Manager], May 10, 2021 (Cyberspace Admin. of China) (China), www.cac.gov.cn/2021-05/10/c_1622225924090817.htm; Guanyu Douyin Deng 105 Kuan App Weifa Weigui Shouji Shiyong Geren Xinxi Qingkuang De Tongbao (关于抖音等105款App违法违规收集使用个人信息情况的通报) [Announcement on the Illegal Collection and Use of Personal Information by 105 Apps Including Douyin], May 21, 2021 (Cyberspace Admin. of China 2021) (China), www.cac.gov.cn/2021-05/20/c_1623091083320667.htm; Guanyu Keep Deng 129 Kuan App Weifa Weigui Shouji Shiyong Geren Xinxi Qingkuang De Tongbao (关于Keep等129款App违法违规收集使用个人信息情况的通报) [Announcement on the Illegal Collection and Use of Personal Information by 84 Apps Including Keep], June 11, 2021 (Cyberspace Admin. of China) (China), www.cac.gov.cn/2021-06/11/c_1624994586637626.htm;

[172] Guojia Wangxinban Yifa Yuetan Chufa Xinlang Weibo (国家网信办依法约谈处罚新浪微博) [Cyberspace Administration of China Interviewed and Punished Sina Weibo in accordance with the Law], Dec. 14, 2021 (Cyberspace Admin. of China) (China), www.cac.gov.cn/2021-12/14/c_1641080795548173.htm; Guojia Wangxinban Yifa Yuetan Chufa Douban Wang (国家网信办依法约谈处罚豆瓣网) [Cyberspace Administration of China Interviewed and Punished Douban in accordance with the Law], Dec. 2, 2021 (Cyberspace Admin. of China) (China), www.cac.gov.cn/2021-12/02/c_1640043205326056.htm.

[173] Guojia Hulianwang Xinxi Bangongshi Deng Qi Bumen Jinzhu Didi Chuxing Keji Youxian Gongsi Kaizhan Wangluo Anquan Shencha (国家互联网信息办公室等七部门进驻滴滴出行科技有限公司开展网络安全审查) [Seven Authorities Including the State Internet Information Office Enters Didi Chuxing Technology Co Ltd to Conduct Cybersecurity Review], July 16, 2021 (Cyberspace Admin. of China) (China), www.cac.gov.cn/2021-07/16/c_1628023601191804.htm.

[174] Shichang Jianguan Zongju, Zhongyang Wangxinban, Shuiwu Zongju Lianhe Zhaokai Hulianwang Pingtai Qiye Xingzheng Zhidao Hui (市场监管总局、中央网信办、税务总局联合召开互联网平台企业行政指导会) [State Administration for Market Regulation, Cyberspace Administration of China, and the State Taxation Administration Jointly Hold Administrative Guidance Meeting of Internet Platform Businesses], STATE ADMIN. FOR MKT. REG. (Apr. 13, 2021), www.samr.gov.cn/xw/zj/202104/t20210413_327785.html.

paign to ban spy cameras and hidden-camera videos.[175] Multiple state authorities have also come together to adopt a number of regulations and other measures targeting the internet and technology sector, including requiring digital platforms with the personal information of more than one million users to undergo cybersecurity review before listing overseas,[176] defining the necessary personal information that mobile apps can collect from their users,[177] regulating the use of algorithmic recommendations by internet and technology companies,[178] managing automotive data security,[179] and protecting the rights of drivers working for ride-hailing and food delivery digital platforms.[180] Although the regulators and state authorities involved in the enforcement cam-

---

[175] Zhongyang Wangxinban, Gongye He Xinxi Hua Bu, Gongan Bu, Shichang Jianguan Zongju Guanyu Kaizhan Shexiangtou Toukui Deng Heichan Jizhong Zhili De Gonggao (中央网信办, 工业和信息化部, 公安部, 市场监管总局关于开展摄像头偷窥等黑产集中治理的公告) [Announcement of the Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, and the State Administration for Market Regulation on the Centralized Governance of Spy Cameras and other Black Market Products], June 11, 2021 (Cyberspace Admin. of China) (China), www.cac.gov.cn/2021-06/11/c_1624994108997096.htm.

[176] Wangluo Anquan Shencha Banfa (网络安全审查办法) [Cybersecurity Review Measures] (promulgated by State Internet Info. Off., Nat'l Dev. and Reform Comm'n, Ministry of Industry and Info. Tech., Ministry of Public Security, Ministry of State Security, Ministry of Fin., Ministry of Com., People's Bank of China, State Admin. for Mkt. Reg., State Admin. of Radio and Television, China Sec. Reg. Comm'n, State Secrecy Admin., and State Cryptography Admin., Jan. 4, 2022, effective Feb. 15, 2022) (China).

[177] Changjian Leixing Yidong Hulianwang Yingyong Chengxu Biyao Geren Xinxi Fanwei Guiding (常见类型移动互联网应用程序必要个人信息范围规定) [Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Apps] (promulgated by the State Internet Info. Off., Ministry of Industry and Info. Tech., Ministry of Public Security, and State Admin. for Mkt. Reg., Mar. 12, 2021, effective May 1, 2021) (China).

[178] Hulianwang Xinxi Fuwu Suanfa Tuijian Guanli Guiding (互联网信息服务算法推荐管理规定) [Provisions on Regulating Algorithmic Recommendations for Internet Information Services] (promulgated by State Internet Info. Off., Ministry of Industry and Info. Tech., Ministry of Public Security, and State Admin. for Mkt. Reg., Jan. 4, 2022, effective Mar. 1, 2022) (China).

[179] Qiche Shuju Anquan Guanli Ruogan Guiding (Shixing) (汽车数据安全管理若干规定(试行)) [Provisions on the Management of Automotive Data Security (Trial)] (promulgated by the State Internet Info. Off., Nat'l Dev. and Reform Comm'n, Ministry of Industry and Info. Tech., Ministry of Public Security, and Ministry of Transport, Aug. 16, 2021, effective Oct. 1, 2021).

[180] Guanyu Luoshi Wangluo Canyin Pingtai Zeren Qieshi Weihu Waimai Songcan Yuan Quanyi De Zhidao Yijian (关于落实网络餐饮平台责任切实维护外卖送餐员权益的指导意见) [Guiding Opinions on Implementing the Responsibilities of Online Catering Platforms and Effectively Protecting the Rights and Interests of Food Delivery Workers] (promulgated by State Admin. for Mkt. Reg., Cyberspace Admin. of China, Nat'l Dev. and Reform Comm'n, Ministry of Public Security, Ministry for Human Resources and Social Security, Ministry of Com., and All-China Fed'n of Trade Unions, July 16, 2021) (China); Guanyu Jiaqiang Jiaotong Yunshu Xin Yetai Congye Renyuan Quanyi Baozhang Gongzhuo De Yijian (关于加强交通运输新业态从业人员权益保障工作的意见) [Opinions on Strengthening the Protection of the Rights and Interests of Employees of New Forms of Transportation] (promulgated by the Ministry of Transport, Cent. Propaganda Dep't, Cyberspace Admin. of China, Nat'l. Dev. and Reform Comm'n, Ministry of Public Security, Ministry of Human Resources and Social Security, State Admin. for Mkt. Reg., All-China Fed'n of Trade Unions, Dec. 1, 2021) (China).

paign were wide-ranging, and the concerns addressed were different and overlapping, these efforts to assert, protect, and even potentially expand regulatory turfs through the campaign do not appear to have been met with political or bureaucratic resistance and challenge from other regulators and state authorities.

At the time of writing, the Chinese government has signaled that it will slow down the intensity of its regulatory activities involving internet and technology companies in China.[181] However, even if the vigor of enforcement activity targeting particular companies subsides, internet and technology companies in China will not simply return to the loose regulatory environment that they had previously enjoyed. Their activities are now more strictly and comprehensively regulated by the new and updated legal and regulatory measures adopted during the campaign, more regulations will also be needed to continue to implement the data governance laws, and there will be greater enforcement of the data governance laws.

Furthermore, not only did the campaign boost the political and enforcement powers of the CAC and SAMR, these two regulators now have a stronger mandate to supervise and regulate internet and technology companies. In particular, the improvements made to the legal and institutional framework for competition law and the strengthening of the SAMR's powers will make it easier for China's competition laws to be enforced to address competition issues involving data. Therefore, even with the growing enforcement of the data governance laws by other regulators and the potential for bureaucratic and regulatory conflicts, resistance, and tussles with them, it is likely that China's competition laws will be applied more often to regulate data.

B. POTENTIAL INFLUENCE OF DATA GOVERNANCE CONSIDERATIONS ON COMPETITION LAW ENFORCEMENT

If competition law is applied to data and data practices, the goals, interests, and concerns relating to data governance—some of which are not traditionally associated with competition—will nonetheless likely be relevant in the competition law decision-making process. As shown in Part II, the competition law framework itself, as well as the way that the courts and competition authorities have interpreted and applied the AUCL and AML, allow for the con-

---

[181] Yaling Jiang & Tracy Qu, *China's Regulatory Storm May Soon Subside for Big Tech Firms After Xi Jinping's Right-Hand Man Calls for Order and Transparency*, S. CHINA MORNING POST (Mar. 18, 2022); *Liu He Zhuchi Guowuyuan Jinrong Wei Huiyi Yanjiu Dangqian Xingshi* (刘鹤主持国务院金融委会议研究当前形势) [Liu He Holds State Council Finance Committee Meeting to Study the Current Situation], XINHUA (Mar. 16, 2022), www.news.cn/politics/leaders/2022-03/16/c_1128475467.htm; *see also* Rui Ma et al., *Is Beijing Changing Tack on Big Tech? A ChinaFile Conversation*, CHINAFILE (May 19, 2022), www.chinafile.com/conversation/beijing-changing-tack-big-tech.

sideration of some data security and personal information protection issues in certain situations. Further, in October 2021, the SAMR released draft guidelines to classify digital platforms and set out their responsibilities.[182] In addition to anti-monopoly, unfair competition, and consumer protection, the draft guidelines outline the obligations of digital platforms relating to, *inter alia*, cybersecurity, data security, privacy and personal information protection, workers' rights, environmental protection, and tax. Most of these matters are not strictly within the SAMR's remit as the market regulator. Although guidelines are not legally binding, they do outline the approach that the SAMR intends to take in carrying out its mandate and enforcing laws against digital platforms. These draft guidelines suggest that the SAMR will approach the regulation of digital platforms from a more holistic perspective that might incorporate considerations beyond competition and consumer concerns, which in turn will likely shape its enforcement of the competition laws.

Additionally, data governance principles, concerns, and goals could be brought into competition law through the consultation that is required as part of bureaucratic decision-making in China. When taking action under the AML or AUCL, the SAMR will usually need to consult with other relevant state authorities to obtain their comments or views on a particular matter and have them agree to and sign off on the outcome.[183] For example, it would not be unusual for the SAMR to consult the CAC and MIIT on an investigation or merger review in the internet and technology sector. It is through this process of consultation that other state authorities could, if they chose, bring their own interests and concerns into the competition law decision-making process and seek to influence the competition law outcome. In the past, there have been cases where consultation with other state authorities did appear to affect decision-making under the AML and its enforcement.[184] For example, some merger remedies seemed to be more directed at addressing the concerns of consulted government departments rather than the potential anticompetitive

---

[182] Hulianwang Pingtai Fenlei Fenji Zhinan (Zhengqiu Yijian Gao) (互联网平台分类分级指南 (征求意见稿)) [Guidelines for Classifying Internet Platforms (Draft for Comments)] (released by the State. Admin. for Mkt. Reg., Oct. 29, 2021) (China); Hulianwang Pingtai Luoshi Zhuti Zeren Zhinan (Zhengqiu Yijian Gao) (互联网平台落实主体责任指南 (征求意见稿)) [Guidelines for Implementing the Main Responsibilities of Internet Platforms] (released by the State. Admin. for Mkt. Reg., Oct. 29, 2021) (China).

[183] Failure to undertake proper consultation with relevant state authorities could expose the SAMR's decision to challenge from within the bureaucracy; *see also* Jingyingzhe Jizhong Shencha Zhanxing Guiding (经营者集中审查暂行规定) [Interim Provisions on the Review of Concentrations Between Business Operators] (promulgated by the State Admin. for Mkt. Reg., Oct. 23, 2020, effective Dec. 1, 2020) (China), art. 23; Guowuyuan Gongzuo Guize (国务院工作规则) [State Council Work Rules] (promulgated by the State Council, June 25, 2018) (China).

[184] NG, POLITICAL ECONOMY, *supra* note 145, at 247–59.

effects.[185] The lack of transparency in the administrative decision-making and governance system in China does, however, make it somewhat difficult to know how decision-making proceeds, who participates, and how various matters are balanced and coordinated.

Even if data governance matters do enter the competition law decision-making process, this does not necessarily mean that competition concerns will not be properly considered, overlooked, or not addressed. The SAMR still needs to carry out its mandate and responsibilities as the competition regulator, and the SAMR and the courts need to determine how the anti-monopoly or unfair competition conduct should be addressed from a competition law standpoint. The extent to which data governance-related interests, concerns, and objectives can be addressed within the ambit of China's competition laws remains somewhat constrained by those competition law analytical frameworks and norms.

This is evident from the body of published competition law decisions to date, as they are clearly framed and grounded in what is regarded as standard competition law language and analysis. For example, the AML decisions are, on the whole, in keeping with international competition law norms and approaches taken by other jurisdictions. This has occurred even in cases where it seems that non-competition considerations did influence outcomes. In fact, non-competition factors were not usually referenced in AML decisions, even when they were allowed to be considered under the AML.[186] On the one hand, these decisions demonstrate that, where conduct has come under the scrutiny of China's competition laws, the competition authorities and courts have been mindful that their decisions need to be justifiable from a competition law analytical perspective. At the same time, however, this has obfuscated the consideration and influence of non-competition factors in decision-making under competition law, posing issues for transparency. This makes it more difficult to understand when and how non-competition factors such as data governance-related matters will be considered and addressed by the SAMR and the Chinese courts under the rubric of competition law.

IV. CONCLUSION

In China, like in many other countries around the world, individuals, businesses, and the state are increasingly aware of the value of—and opportunities and risks associated with—data, especially with the growth of the internet, digital economy, and related technologies. The Chinese government looks at data through a kaleidoscopic lens—it recognizes the political and security implications of data and regards data to be economic (and at times, public) assets

---

[185] *Id.* at 248–50.

[186] Ng, *State Interest*, *supra* note 145, at 299–303.

that have benefits for China's economic and development goals. China is developing an increasingly sophisticated data governance regime that reflects this myriad of public and private concerns, goals, and interests. The Chinese government regulates the access, use, and flow of data and fosters the development of the internet, digital economy, and data and technology industries, with the overarching aim of facilitating state influence and control over relevant companies, sectors, and data. The regulation of data, for example, has been critical in the recent campaign targeting internet and technology companies.

Competition law will increasingly play a larger and more meaningful role in regulating data in China. The enforcement campaign against internet and technology companies, political support from China's leaders for competition law enforcement, an updated competition law framework that is better equipped to address anti-monopoly and unfair competition conduct issues arising in the digital economy, and improved institutional arrangements all provide the SAMR and private litigants with the ability and incentive to enforce China's competition laws to target the data and data practices of internet and technology companies, especially digital platforms. The jurisdictional overlap between data regulation and competition law—and ensuing web of stakeholders, objectives, concerns, and interests—does, however, complicate matters as they will most likely constrain the role and application of competition law to data.

Beyond the data and conduct falling within the formal scope of both legal frameworks, the relationship between these two spheres of regulation is shaped by the political power of and relationships between different stakeholders, their goals, concerns, and interests in data, and the broader governance and political environment and dynamics. This article has argued that China's competition laws are feasible avenues through which to regulate data where the data and conduct relate to industrial policy, economic and social development, and privacy and personal information protection matters, whereas if the data implicate national and public security, that would probably be more directly handled by the data governance laws and not the competition laws.

The fact that various interests, concerns, and goals and political considerations influence the regulatory environment and legal enforcement for data regulation and competition regulation is not something that occurs only in China. The changing political tide against internet and technology companies and the centrality of competition law enforcement and reform to discussions about how best to regulate these companies are occurring in many countries around the world. By significantly stepping up its focus and activities on internet and technology companies, the SAMR joins the ranks of many other competition regulators. Nonetheless, the embeddedness of the state and its interests, con-

cerns, and goals in competition law, markets, and data governance does reflect the philosophy in China about the more assertive role of the state in the market, economy, and society more broadly, as well as its socialist political and legal system.[187]

[187] *See also, e.g.*, Barry Naughton, *What's Behind China's Regulatory Storm*, WALL ST. J. (Dec. 12, 2021).