Chinese Data Protection in Transition

A Look at Enforceability of Rights and the Role of Courts

Hunter Dorwart

Note this draft paper has been accepted to the 2022 Computers, Privacy, and Data Protection (CPDP) conference and awaits approval for publication. Please do not distribute or cite.

Abstract*: In recent years, the Chinese government has solidified its data protection framework through a series of laws and regulations to address the social, economic, and political challenges posed by the digital age. Many of these policy instruments explicitly recognize data subject rights and set forth numerous obligations for entities processing personal information—a trend seen in other regulatory approaches around the world. While much of the academic community has focused on the implementation of this larger framework through China's top-down, centrally administered institutions, little discussion has turned to the role of courts in enforcing these rights at the local level. This paper attempts to address that gap by examining recent privacy litigation in China and situating it within China's larger governance structure. While privacy litigation is increasing, such litigation will likely play a secondary and complementary role to efforts undertaken by other central institutions. Nonetheless, courts in China will likely help resolve smaller-scale disputes on the local level where enforcement from the top proves challenging. Unraveling this role puts the international data protection community one step forward in understanding the complexities of data privacy enforcement in China.*

I. INTRODUCTION

In recent years, data protection and governance has become an important topic for policymakers in China.[1] While debates around Internet governance have circulated in the country for quite some time, an elevated sense of urgency now permeates much of the discourse. Indeed many stakeholders in government, industry, and academia agree that the widespread collection and use of data now operates as a central prism through which the government can realize its societal and economic goals.[2] Communication networks enable individuals to connect with one another at an unprecedented scale, streamlining operational processes and generating new sources of value for individuals and companies.[3] Advances in cloud computing and fifth-generation (5G) low latency networks promise to enable a range of cybernetic industrial activities, revolutionize global logistics, and introduce applications related to connected vehicles and smart cities.[4] Key to this is transforming China into the next technological and scientific world leader – a priority outlined extensively in the country's 14th Five Year Plan (FYP).[5]

This priority underscores the tremendous economic growth the country has experienced in the past two decades. Such growth is now clearly visible in the online realm. By 2025, estimates indicate that China's internet population will reach 1.14 billion.[6] The country boasts some of the largest Internet companies by revenue and market capitalization in the world, including JD.com, Alibaba, Tencent, and Baidu.[7] In the telecommunications industry, Huawei is now the largest

[1] As discussed below, conceptual terminology on the matter differs slightly between the U.S. and China. While the term "platform economy" is widely used in both countries to discuss economic processes characterized by data-driven, online transactions and digital intermediaries, there is disagreement as to what constitutes a "platform" and whether it should be separated from similar concepts such as aggregators or gatekeepers. Chinese scholars seem to embrace "platform economy" more readily than their American or European counterparts. For a general overview see e.g., Chuanman You, "Law and Policy of Platform Economy in China" *Computer Law & Security Review*, No. 39 (2020); William Chou, Iris Li & Lingxiao Zhang, "New Governance of the Platform Economy" *Deloitte* (2020); Tim Wu, "Ben Thompson's 'Stratechery'" *Medium* (2020).

[2] "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035" *Xinhua News Agency* (Mar. 12, 2021), https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf

[3] See Gerald C. Kane et al., "Aligning the Organization for its Digital Future" *MIT Sloan Management Review* (2016).

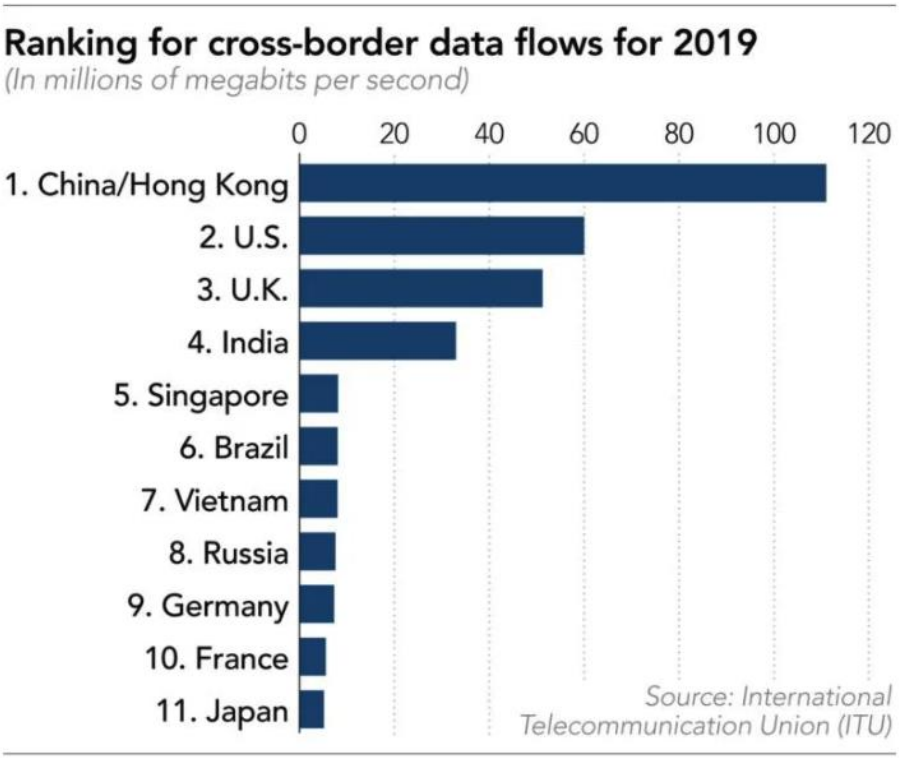
[4] S. Aslam & H. Sami Ullah, "A Comprehensive Review of Smart Cities Components, Applications, and Technologies Based on Internet of Thing" *Arxiv* (2020), https://arxiv.org/abs/2002.01716; Leonardo Guevara & Fernando Auat Cheein, "The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems" *Sustainability* (2020), https://www.mdpi.com/2071-1050/12/16/6469/pdf

[5] See *supra*, note 2.

[6] Longmei Zhang & Sally Chen, "China's Digital Economy: Opportunities and Risks," Working Paper 19/16, *Int'l. Monetary Fund* 5 (2019) https://www.imf.org/~/media/Files/Publications/WP/2019/wp1916.ashx

[7] Sean Ross, "5 Biggest Chinese Software Companies" *(CHL, TCEHY)*, *Investopedia* (Feb. 25, 2020), https://www.investopedia.com/articles/markets/032616/5-biggest-chinese-software-companies-chl-tcehy.asp

provider of equipment with a 31% global market share in 2020.[8] Chinese universities produce millions of STEM graduates degree a year, with thousands of students flocking to overseas universities for similar programs.[9] Major cities in China have become world-class technology hubs, attracting a total of $2.2 trillion of R&D in 2019 for technologies including artificial intelligence, robotics, and autonomous vehicles.[10] China's e-commerce now accounts for roughly 35% of total retail sales in the country, with a market size expected to reach $5.6 trillion in recent years.[11] More data flows across China's border than both the U.S. and the U.K. combined and is projected to increase substantially in the near future.[12]



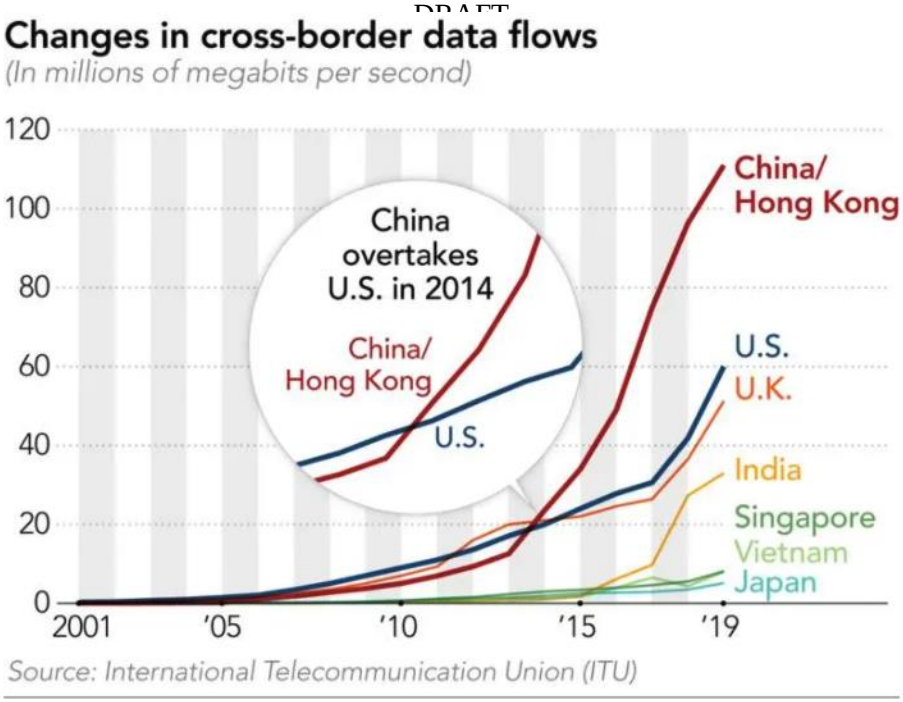
[8] Stefan Pongratz, "Key Takeaways – The Telecom Equipment Market 1H20," Dell'Oro Group (2020), https://www.delloro.com/key-takeaways-the-telecom-equipment-market-1h20/

[9] See Katherine Stapleton, "China Now Produces Twice as Many Graduates a Year as the US," *World Economic Forum* (2017) (finding that China graduated 4.7 million STEM graduates in 2016) https://www.weforum.org/agenda/2017/04/higher-education-in-china-has-boomed-in-the-last-decade; but cf. National Science Foundation Science & Engineering Indicators 2018 (challenging the WEF numbers by stating that China classifies STEM broadly than other countries).

[10] "Rising Innovation in China: China Innovation Ecosystem Development Report 2019," *Deloitte China* 7-8 (2019) https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/innovation/deloitte-cn-innovation-china-innovation-ecosystem-report-en-191101.pdf

[11] Min Jiang, "Cybersecurity Policies in China," in *CyberBRICS: Cybersecurity Regulation in the BRICS Countries* 200 (2020).

[12] https://asia.nikkei.com/Spotlight/Century-of-Data/China-rises-as-world-s-data-superpower-as-internet-fractures



Yet the realization of China's goals has not come without obstacles. On the one hand, the rapid transition to the online world has also resulted in a multitude of harms to individuals and consumers in the country. Government authorities have struggled to combat deceptive data practices including unfair algorithmic decision-making, unauthorized disclosures, and profiling through online tracking.[13] The rapid growth of platforms through network effects and data aggregation has given rise to antimonopoly concerns that have led to a series of recent enforcement targeting nearly every aspect of the digital economy.[14] This has generated a growing public backlash against the widespread collection, use, and disclosure of personal information by the largest tech firms in China.[15] Indeed, a series of high-profile data breaches and cases of personal information abuse have raised awareness in China of the need for broad data protection in the digital economy and strengthened demands for privacy from intrusive technologies such as facial recognition, app-tracking software, and automated processing.[16]

[13] Han Wei, "Baidu Sued Over Claim It Illegally Obtained Users' Data" *Caixin* (2018); Qin Jianhuang, Qian Tong & Han Wei, "Cover Story: The Fight Over China's Law to Protect Personal Data" *Caixin* (2020).
[14] See e.g., Hunter Dorwart & Gabriela Zanfir-Fortuna, "Spotlight on the Emerging Chinese Data Protection Framework: Lessons Learned From the Unprecedented Investigation of Didi Chuxing" *Future of Privacy Forum* (2021), https://fpf.org/blog/spotlight-on-the-emerging-chinese-data-protection-framework-lessons-learned-from-the-unprecedented-investigation-of-didi-chuxing/;
[15] Qin, Qian & Han *supra*, note 13.
[16] One notorious case, which sparked public outcry, concerned a high school student in Shandong province that died of a heart attack after being successfully targeted by phone scammers who illegally obtained her information from a poorly administered school database. Another in 2018 saw a consumer-protection organization sue Baidu in China for collecting users' information without consent. Lastly, a professor in Hangzhou received broad public support in

On the other hand, such technologies have also redefined the contours of power on a global stage. Chinese leaders increasingly view technology through the lens of national security and related interests.[17] As a result, policymakers in China have formulated government strategies to minimize dependency on international supply chains, build self-reliance on domestic capabilities, and develop resiliency in sourcing critical technological inputs.[18] From semiconductors and software to critical infrastructure, powerful interest groups within the country now perceive technological interdependency as undermining national interest and generating exploitable vulnerabilities in information technology (IT) networks.[19]

In partial response to these obstacles, the Chinese government has adopted a series of laws and regulations to better solidify the country's legal framework for data governance. Like other jurisdictions around the globe, data protection and privacy form a crucial pillar in this larger legal framework, especially when it comes to mitigating consumer harm and ensuring personal dignity in the digital age, two goals explicitly recognized (if not always followed) by Chinese leaders.[20] China promulgated the Cybersecurity Law in 2017, which mandates that network operators comply with a series of security requirements including those related to personal information processing, compiled a Civil Code in 2020 containing a chapter on personality rights involving privacy and data protection, and adopted both the Data Security Law and the Personal Information Protection Law (PIPL) in 2021. Additionally, multiple ministries within China's vast bureaucracy have formulated their own regulations and industry standards, which deal primarily with sector-specific issues and clarify key aspects of the laws mentioned above.[21]

Both the Civil Code and the PIPL create enforceable data subject rights modelled explicitly off the EU's General Data Protection Regulation (GDPR) and impose obligations on data controllers to enforce these rights when requested.[22] Moreover, under Chinese law, public bodies

---

bringing a zoo to court to challenge its use of facial recognition technologies in its parks. See Qin Jianhuang, Qian Tong & Han Wei *supra*, note 12.

[17] Ambak Kak & Samm Sacks, "Shifting Narratives and Emergent Trends in Data-Governance Policy: Developments in China, India, and the EU" *Policy Memo* (2021), p. 6.

[18] Ryan Fedasiuk, Emily Weinstein & Anna Puglisi, "China's Foreign Technology Wish List" *Center for Security and Emerging Technology* (2021), https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-Foreign-Technology-Wish-List.pdf.

[19] *Infra*, Section II.

[20] Emmanuel Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?" *Penn State Journal of Law & International Affairs* Vol. 8, No. 1 (2020).

[21] See Kak & Sacks *supra*, note 17 p. 10.

[22] See *infra*, Section II(A).

must also comply with these requirements and follow the principles of transparency, fairness, and accountability—a process well-aligned with internationally recognized norms.[23] While the laws serve other interests besides protecting individuals, the emergence of this legal architecture underscores the government's desire to empower such individuals to enforce their data subject rights and promote a healthier data ecosystem in the future.[24]

Like other aspects of governance in China, privacy and security regulation has largely been realized through centralized, top-down institutions. Analysts focus heavily on the formulation of laws, regulations, and industry standards for signals of market risk while emphasizing enforcement actions to explain changes in corporate behavior. They do so for good reason—China's legal system places a great deal of importance on the central bureaucracy to accomplish its regulatory goals and often relies on informal relationships between government regulators and industry leaders to effectuate larger policies. However, ignored in this focus is the role of courts in China and how they will guide the enforceability of data protection rights on a national level. Given the country's unique political and legal system, many questions remain as to the specifics of enforceability. How will individuals in China meaningfully enforce their rights when faced with a complex set of institutional and political barriers? To what extent will the legal system play a role in this process and what is the best way to characterize this role? Are individuals in China exercising their rights through courts or other forms of judicial adjudication? Do courts have the authority and the ability within China to significantly change the data processing behaviors of local governments or corporate entities? Does Chinese data protection law meaningfully constrain the power of public bodies?[25]

This paper seeks to address these issues by offering an analysis of privacy and data protection litigation in China. First, it examines the relevant provisions in both the PIPL and the recently compiled (编纂) Civil Code (2020) that sets forth data protection rights and obligations for entities processing personal information. Second, it analyzes recent privacy case law in Chinese courts and attempts to identify notable trends in the enforceability of data subject rights on the grassroots level. Last, it contextualizes these trends within the overall structure of China's governmental system by addressing the structural limitations of litigation in the country as a

[23] Ibid.
[24] *Infra* section II(A).
[25] See *infra* section IV.

mechanism for broad policy implementation as well as the complexities behind enforcing rights in the civil context.

While data privacy litigation is increasing in both scale and frequency, it will most likely play a backseat role in China's overall regulatory system. China's unique governance system creates the impression that when courts act, they do so largely with the approval of the central government or within an accepted governance framework. In other words, legal compliance culture revolves around understanding what the central authorities want, who often formulate regulatory guidelines before the passage of any law or the announcement of any enforcement action.[26] Indeed, this system demands that lawyers and analysts trained in other models of legal organization such as those in the United States or European Union reevaluate their preconceptions about the appropriate legal structure of government and the role of the judiciary in that structure. Instead, properly contextualizing China's legal system within the overall regulatory structure of the government requires approaching China on its own terms.[27]

Nonetheless, while the central government in China will take the lead in targeting large-scale market participants for their data privacy and protection abuses, courts will still play a role in resolving smaller-scale disputes, offer private litigants the ability to hold certain entities accountable, and even bring cases against larger actors through the civil public interest litigation vehicle. They may also help fill in the details of certain regulations or industry standards issued from ministries by providing guidance on ambiguous terms or the requirements for compliance.

This paper does not attempt to provide an exhaustive overview of privacy litigation in China, nor does it offer a comprehensive model through which to view developments in Chinese law regarding data protection. Rather it aims to present a useful framework to address these concerns and explore ways in which recent litigation data fits within the larger trends related to data governance. Due to this more tailored goal, this paper does not address some of the notable issues that characterize the problems of legal reform in China such as the execution of civil judgments, the lack of consistency or uniformity in the structure of the bureaucracy, or the subordination of courts to other institutions. Nor does it focus on other notable laws in Chinese data governance that deal primarily with security and data classification issues.

[26] Paul Triolo et al. "China's Cybersecurity Law One Year On: An Evolving and Interlocking Framework," *New America*, https://d1y8sb8igg2f8e.cloudfront.net/documents/Chinas_Cybersecurity_Law_One_Year_On.pdf
[27] Jingjing Liu, "Overview of the Chinese Legal System," Vol. 1 *Environmental Law Institute* (2013).

Section II presents an overview of how data protection and privacy has evolved in China with a particular focus on the provisions of the PIPL and the Civil Code that touch upon data subject rights. Section III, in turn, delves into the case law regarding these provisions and highlights some notable takeaways from the data. Section IV offers a synthesized account of the roles of courts for data protection in China and addresses some of the key questions facing their efficacy in relation to other governance institutions. Section V provides concluding remarks.

II. OVERVIEW OF PERSONAL DATA PROTECTION IN CHINA

The development of data privacy in China presents a long and complicated history.[28] Mirroring the profound socio-technological developments in China at the end of the 20th century, conceptions of privacy in the 1980s began to expand to accommodate the new demands of the transition to a market-based mixed economy.[29] While not always directly visible, Chinese scholars at the time took great care to document the changes on the local level and often framed their analyses through psychological terms and sociological concepts.[30] Such studies highlighted a variety of changing social expectations that led to the emergence of a "self-consciousness" right of privacy such as declining an interlocutor's questions about a sensitive topic, conceptualizing privacy beyond its limited definition in the common word *yinsi* (阴私) (i.e., a shameful secret) and expecting privacy in new circumstances around the family and one's education.[31] Legal scholars similarly noted important changes within the law that reinforced privacy protection in certain circumstances.[32]

With the popularization of the Internet in the 1990s, privacy problems around data began to emerge, both as a matter of domestic regulation and foreign engagement.[33] The rapid spread of

[28] Yehan Huang & Mingli Shi, "Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law" *DigiChina* (2021), https://digichina.stanford.edu/news/top-scholar-zhou-hanhua-illuminates-15-years-history-behind-chinas-personal-information
[29] Lu Yao Huai, "Privacy and Data Privacy Issues in Contemporary China" Vol. 7 *Ethics and Information Technology* (2005), p. 7.
[30] See e.g., D.-L. Liu. "On Privacy and Right to Privacy" Vol. 8 *Social Science* (2003); R.-F. Li and Y. Na. "A Philosophical Reflection on the Loss of Privacy." Vol. 5 *Science, Technology and Dialectics* (2003), 38–41. Both citations come from Lu *supra*, note 141.
[31] See e.g., Zheng Hansheng, "21st Century Chinese: Time, Competition, and Privacy" (二十一世纪的中国人—时间，竞争，隐私), *China Soft Science*, Vol. 2 (1994) pp. 47-49. 《中国软科学》(1994 年第 2 期第 47-49 页)
[32] C.-M. Zhou and C. Wen-Qu. Right to Data Privacy and Legal Protection of It." *Lawyers World* (2001).
[33] X.-B. Zhang, "The Development of IT and the Protection of Right to Privacy," *Law and Social Development* (1996), pp. 16-25.

e-commerce introduced new risks for consumer protection and facilitated a market for all types of personal and confidential information.[34] In addition, communication networks provided a new infrastructure for the dissemination of information that greatly increased the possibility of connectivity and information sharing.[35] Chinese leaders quickly saw the immense potential of Internet technologies not only for the digitalization of the market economy but also for China's capacity to lead innovation and secure the promise of building a robust middle class of consumers.[36] Over time, these goals became more explicitly tied to the Chinese government's larger developmental and global engagement objectives, especially in the post-2008 period.[37]

However, these leaders also recognized that if unregulated, global communication technologies could undermine the structures of social, economic, and political stability.[38] In fact, the Chinese government was one of the first in the world to place special attention on *the role of the state* in regulating the ICT industry.[39] In the late 1990s, it developed comprehensive censorship protocols early on, initiated a nationwide network-security and traffic management system through the Golden Shield Project (金盾工程), and operationalized both offensive and defensive cyber capabilities.[40] It also laid the foundation for state regulation of Internet companies through strengthening the country's licensing and certification mechanisms.[41] The Chinese government accomplished this through a combination of laws, regulations, and technical standards with the State Council playing a leading role in the coordination of lower-level operational departments.[42]

---

[34] See Huang & Shi *supra*, note 28.
[35] See Haiping Zheng, "Regulating the Internet: China's Law and Practice," 4 *Beijing Law Review* 4 (2013) (discussing early Chinese regulations of the Internet).
[36] While these developmental goals have changed in nature and context over time, there is a striking continuity between the early rationalizations of what the Internet could provide, and more recent policy iterations outlined in the 14th Five Year Plan (2020-2025). Severine Arsene, "China, Internet Governance and the Global Public Interest" *A New Responsible Power China* (2018), p. 72..
[37] Shulin Gu & Bengt-Ake Lundvall, "China's Innovation System and the Move Towards Harmonious Growth and Endogenous Innovation," 8 *Innovation: Organization and Management* (2006).
[38] Lu Chuanying (鲁传颖), Zhuquan Gainian de Yanjin Jiqi Zai Wangluo Shidai Mianlin de Tiaozhan (主权概念的演进及其在网络时代的挑战) [Evolution of the Concept of Sovereignty in the Challenges of the Internet Age] 1 Guoji Guanxi Yanjiu (国际关系研究) [International Relations Studies] 75-77 (2014).
[39] Yang Rongjun (杨嵘均), Lun Wangluo Kongjian Zhili Guoji Hezuo Mianlin de Nanti Jiqi Yingdui Celüe 伦王国空间治理国际合作面临的及其应对策略) [On Problems and Strategies of International Cooperation in Cyberspace Governance], 13 Guangxi Shifan Daxue Xuebao (廣西師範大學学报) [Guanxi Normal Uni. J. of Soc. Studies) 79 (2014).
[40] Sonali Chandel et al., "The Golden Shield Project of China: A Decade Later," *Institute of Electrical and Electronics Engineers* (IEEE) (2019), https://ieeexplore.ieee.org/document/8945933.
[41] Wei Lu et al., "Internet Development in China," Vol. 28 *Journal of Information Science* (2002).
[42] Ibid.

To be sure, China was not the only country to prioritize regulation over the Internet and communication technologies. Indeed, building institutional and technical capacity in this space was a challenge faced by nearly all countries that had access to the technologies, even if such access was uneven due to historical and developmental conditions.[43] Yet what made China's approach unique was its emphasis on the priority of *national* competence over the Internet space and the clear demarcation of Chinese sovereignty from a transnational system of interconnected networks largely overseen by non-governmental entities.[44]

China recognized early on the importance of data protection in this ecosystem of technologies. While debates around privacy began to change in the late 1990s, personal information protection issues took on an independent direction from privacy and often intertwined with larger Internet governance issues like network traffic monitoring, cyber incident reporting, critical infrastructure management and information security.[45] In 2001, China initiated a legislative process to regulate data protection through the National Informatization Leading Group and the Informatization Office and Export Advisory Committee under the State Council.[46] While these offices formulated many regulations and standards and even proposed a draft Personal Information Protection law in 2005, the Chinese government chose not to promulgate a comprehensive law but rather improved and passed a series of sectoral laws, regulations, and industrial standards to address the issue.[47]

However, in recent years, the Chinese government has recognized the necessity of developing a nationally coordinated framework for data protection and security to strengthen compliance and provide for a more consistent governance and enforcement system.[48] It adopted a

[43] See Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (2010).
[44] To be clear, China's engagement in the international Internet governance debate is far from straightforward. Government leaders have at many times both supported and distanced themselves from international organizations like ICANN and multistakeholder standard-setting bodies like the W3C or the IETF. This dual strategy should come as no surprise as Chinese leaders have emphasized that while needing reform, the current architecture of the Internet serves a useful purpose. See Huang Zhixiong (黄志雄), Wangluo Kongjian Guoji Fazhi: Zhongguo De Lichang, Zhuzhang He Duice (网络空间国际法制：中国的立场主张和对策 (International Law in Cyberspace: China's Status, Position, and Strategy), 32 Yunnan Minzu Daxue Xuebao 137 (云南民族大学学报) [Yunnan Minzu Uni. Press] (2015).
[45] See Huang & Shi *supra*, note 28.
[46] Ibid.
[47] For instance, the Law on the Protection of Consumers (2013) applied nascent data protection expectations on companies while various regulations governed network security and trafficking.
[48] See e.g., Xu Peixi, "A Chinese Perspective on the Future of Cyberspace" *Cyberstability Paper Series* (2021); Rogier Creemers, "The Pivot in Chinese Cybergovernance: Integrating Internet Control in Xi Jinping's China" *China Perspectives* (2015).

comprehensive Cybersecurity Law in 2017, promulgated new rules on data security, classification and exchange through the Data Security Law and recently formulated the Personal Information Protection Law in 2021, as well as an innumerable number of regulations and technical standards on the ministerial level.[49] Additionally, immediately prior to this, the State Council pursued government reform measures that reorganized the competences of the central bureaucracy, refurbished departments within key agencies, and created new supra-ministerial bodies such as the Cyberspace Administration of China (CAC) and the Central Cyberspace Affairs Commission. The goals of these regulatory activities are strikingly like those outlined in a 2003 State Informatization Leading Group report (ZBF. No. [2003]27): to develop a comprehensive network and information system that protects critical technologies through industrial competitiveness, cyber awareness and talent management, and data protection standards.[50]

Part of this larger strategy involves granting individuals data subject rights and imposing obligations on data controllers to respect these rights in their processing activities. This section seeks to provide more detail of how this legal mechanism will work by offering an analysis of two legal instruments—the PIPL and the Civil Code. First, it provides a brief overview of the PIPL with a particular emphasis on the provisions concerning data subject rights and processing obligations. Second, it outlines relevant provisions in China's recently compiled (编纂) Civil Code, which sets forth a new chapter covering data protection rights and significantly improves an older chapter dealing with privacy. This section does not provide an exhaustive analysis of the laws but rather highlights their key takeaways and situates them within the broader context of how data subjects in China enforce rights vis-à-vis data controllers and processors, particularly in the context of legal adjudication via courts and other court-sanctioned methods.

A. The Personal Information Protection Law (PIPL)

On August 20, 2021, the National People's Congress (NPC) adopted China's first comprehensive data protection law—the Personal Information Protection Law (PIPL)—concluding a legislative process that began a year earlier. The PIPL represents one pillar of China's

[49] DigiChina, Stanford Cyber Policy Center. https://digichina.stanford.edu/
[50] "Opinions Concerning Strengthening Information Security Protection Work" *State Informatization Leading Group*, ZBF No. [2003]27), https://chinacopyrightandmedia.wordpress.com/2003/09/07/opinions-concerning-strengthening-information-security-protection-work/

emerging data protection architecture that includes a myriad of other laws, industry-specific regulations, and standards.[51] Additionally, the PIPL explicitly references China's Constitution to provide a firmer legal basis for the law's implementation, particularly around the compilation and enactment of the Civil Code (see below). As such, the PIPL should not be viewed in isolation but rather examined in relation to these other regulatory tools that serve complimentary, albeit different purposes.

Throughout the legislative process, privacy professionals within China played a key role in formulating not only the normative goals of the law but also the principles through which it will be operationalized. These experts drew heavily on the lessons learned from the implementation of the GDPR, which served both as a reference for the PIPL and previous data protection regulations such as the Personal Information Specification of 2018.[52] Indeed, like the GDPR, the PIPL sets forth a range of obligations, administrative guidelines, and enforcement mechanisms with respect to the processing of personal information. For instance, it applies to very broadly defined "personal information" (which carries an element of identifiability), includes lawful grounds for processing after the GDPR model, and applies to the "handling" (处理）of personal information, including the collection of data itself.[53] Notably, the PIPL does not contain a legitimate interest exception and, although other lawful grounds exist, it relies heavily on consent for most processing activities.[54]

Additionally, the PIPL has rules for joint handling with respect to processing on behalf of an original handlers, including agreements that must be put in place before subsequent processing like Article 26 and 28 in the GDPR. The law applies both to the "private" and "public" sectors but contains provisions that exempt compliance when other laws or regulations take priority, including when processing must be done in coordination with state secrecy and confidentiality

[51] For instance, the recently enacted Data Security Law (DSL) sets forth a comprehensive list of requirements regarding the security and transferability of other types of data. It also establishes a "marketplace for data" to enable data exchange and digitalization.

[52] As discussed below more thoroughly, Chinese legal scholars have drawn heavily from texts and codes from European continental law traditions and often look to other models of regulation for guidance and inspiration when contemplating their own drafting. See *supra*, section II(b).

[53] Note the PIPL nor the Civil Code use the concept of "processing" but rather prefer the term "handling." In definitional terms, there is no big difference between handling as understood in Chinese law and processing as understood by the GDPR.

[54] These include where necessary to conclude a contract or for human resource management, where necessary to fulfill statutory duties; where necessary to respond to sudden public health incidents, where done in a reasonable manner for the purpose of news reporting, where the data processed has been publicly disclosed by the data subject, or other circumstances provided in laws or regulations.

requirements.[55] For instance, state organs, critical information infrastructure operators and other handlers reaching a specific volume of processed personal information must meet a broad range of data localization requirements. Specifically, these handlers must comply with certain obligations before transferring data abroad, such as undergoing a security assessment by relevant authorities or complying with a standard contractual clause (SCC).[56] Like the GDPR, the law mandates risk assessments in the form of a personal information impact assessment for specific processing including automated decision-making and handling that could have "a major influence on individuals." Data handlers must also appoint Data Protection Officers (DPOs) in specific situations, which vary depending on the volume of PI processed, and conduct regular compliance training.

This broad convergence with the GDPR indicates that Chinese data protection leaders envision the regulation of data in the country in a manner not too dissimilar from well-established principles in the EU and around the world. Perhaps the most notable convergence of the EU tradition with the Chinese framework comes through the provisions of the PIPL dealing with the rights of the data subject. Under the law, personal information handlers must establish mechanisms to accept and process applications from individuals to exercise their rights. If the information handlers reject the request, they must explain the reason for doing so. The draft law recognizes the following rights:

- Right to *know, decide, refuse, and limit* the handling of their personal information by others, unless laws or regulations stipulate otherwise.
- Right to *access and copy* their personal information in a *timely manner*.
- Right to *correct or complete* inaccurate personal information in a *timely manner*.
- Right to *deletion* if (i) the agreed retention period has expired, or the handling purpose has been achieved; (ii) personal information handlers cease the provision of services; (iii) the individual rescinds consent; (iv) the information is handled in violation of laws, regulations, or agreements.

[55] As discussed below more thoroughly, the distinction between private and public bodies does not readily apply to China's unique political economy, which complicates using the dichotomy to understand Chinese law. Nevertheless, it is important to highlight that the PIPL will restrict the processing activities of certain public bodies, particularly those on the local level. Indeed, one point of this paper is to highlight that the Chinese data protection law does in fact empower Chinese nationals to enforce their rights vis-à-vis public bodies. See *infra* Section III.
[56] The CAC has yet to release these SCCs but is expected to do so by the end of 2021.

- Right to request handlers *explain* their handling rules, including when an individual believes an algorithm has made a decision that affects their interests.
- Right to *data portability* to be defined by subsequent regulations.

As discussed below, the Civil Code also promulgates these rights but goes further in establishing legal requirements specific to privacy and outlines key instances in which a handler can violate a data subject's privacy rights.

However, in contrast to the GDPR, the PIPL serves several other objectives. For examples, it aims to promote and protect China's national security and affirms China's intention to defend its digital sovereignty as articulated through the concept of cyber-sovereignty.[57] Under the law, overseas entities which infringe the rights of Chinese citizens or jeopardize the national security or public interests of China will be placed on a blacklist and any transfers of personal information of Chinese citizens to these entities will be restricted or even barred. China will also reciprocate against countries or regions that take discriminatory, prohibitive or restrictive measures against China with respect to the protection of personal information.[58] These provisions, in part, also reinforce China's ambition to take full part in international protection discussions and actively contribute to setting global standards for technology regulation generally.

Table 1: Comparisons of PIPL to GDPR

	PIPL	GDPR
Right to access data	✓	✓
Right to correct data	✓	✓
Right to delete data	✓	✓
Right to data portability	✓	✓
Right to decline processing	✓	✓
Subject to automated decision*	✗	✓

[57] This refers to the idea that the Internet and the technological networks that make global communication possible should not override the ability of the state to determine its own rules over cyberspace.
[58] Article 43.

Right to explanation	✓	✓
Purpose limitation	✓	✓
** There is some debate as to what the automated decision-making provisions in the PIPL mean in context and practice, especially as they relate to the GDPR's own provisions on the subject matter.*		

B. Compiled Privacy and Data Protection Provisions in the Chinese Civil Code

A year before the adoption of the PIPL, Chinese regulators took one step forward in operationalizing China's data protection architecture by concluding the compilation process of the country's generally applicable Civil Code. On May 28, 2020, the National People's Congress (NPC) approved the Civil Code of the People's Republic of China[59] (中华人民共和国民法) (the Code) after a relatively lengthy compilation process.[60] The Code, which went into effect in 2021, explicitly recognizes the "right to privacy" as one of the personality rights stipulated under Part 4 and includes a chapter on "Privacy and Personal Information Protection."[61] Other categories of rights of personality include life, body and health rights, portrait rights (i.e., right to one's own image), and rights of reputation and honor.[62] As a generally applicable code of civil laws, the provisions concerning privacy and data protection will apply across industries and in all civil and commercial matters. The rights laid out likewise belong to individuals as natural persons, regardless of whether they are consumers, employees, taxpayers, or minors and can be enforced against person or entity that infringes them unless special laws take precedence.

The codification of the Civil Code in China has followed a long historical path that predates the formal creation of the PRC in 1949.[63] While the process of formulating a civil law system faced

[59] Civil Code of the People's Republic of China (2020) [Hereinafter Civil Code]. http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf
[60] Ibid.
[61] Ibid Art. 1032-39.
[62] Ibid.
[63] China has long belonged to the "civil law" tradition, with codification of legal rules dating back to its early dynastic history. Before the "modern" period, China's laws were largely punitive in nature, resulting in the development of criminal legal processes but relatively few laws directly concerning private or civil matters. Towards the end of the Qing dynasty, China's rulers introduced some basic legal concepts eventually codified in a Draft Civil Law and Commercial Law modeled largely from the German and Japanese experience. In the 1930s, the Nationalist Government promulgated a Civil Code modeled directly from the German Civil Code and adopted a series of laws to complement the larger legal architectural design. See Xianchu Zhang, "The New Round of Civil Law Codification in China." Vol. 1, No. 1 *University of Bologna Law Review* (2016).

many political obstacles during the early years of the PRC, there were multiple attempts to develop preliminary draft materials throughout the 1950s and 1960s, modelled on the Soviet Union Civil Code of 1922.[64] After 1978, Chinese leaders recognized the necessity of reforming the legal system to better accommodate civil and commercial matters for China's transition to a semi-market economy but were hesitant in finalizing the civil code due to uncertainties in how it would relate to the competences of the larger administrative structure.[65] In 1986, the NPC promulgated the General Principles of Civil Law as a temporary solution, which set forth a foundation for the development of private law in China, including laws that governed property relations between individuals as private economic actors.[66]

In the transition to a "socialist market economy" in 1993, the NPC initiated another round of codification and by 2002 had introduced a Draft Code.[67] The legislative process faced numerous hurdles at this time as the Draft Code contained a patchwork of existing laws that generated much controversy between members of the drafting group.[68] Indeed, the variety and extent of the various sectoral laws became too unwieldy and presented too many discrete problems for one codification process to solve. At this time, many working groups engaged in broad debates about the appropriate formulation of civil laws and their relationship not only to the practical administration of China's centralized system but also to the country's larger social and economic goals.[69] Many issues lurking in previous rounds of codification resurfaced, such as the extent to which the judicial system should recognize private law and enforce the personality rights enumerated in Draft Code.[70]

[64] Ibid at 6-7.
[65] Liang Hui Xing, "Revisited Certain Issues in Civil Law Codification With Response to De-Codification" *Aisixiang* (2015), http://www.aisixiang.com/data/90909.html
[66] A series of other private laws have been promulgated in this framework including those relating to marriage, tort liability, contract, corporate structure, partnerships, banking, securities, maritime issues, trusts, commercial paper, and intellectual property. See Zhang *supra*, note 63.
[67] Lei Chen & C.H. van Rhee, *Towards A Chinese Civil Code: Comparative and Historical Perspectives* (2002).
[68] Zhang *supra*, note 63.
[69] Sun Xiaolin, "The Debates between Civil and Commercial Law Circles on Adoption of General Principles of Commercial Law Comes Back," *Sina* (2009), http://finance.sina.com.cn/roll/20090113/02585751273.shtml
[70] See e.g., Huixing Liang, "Three Thinking Paths on Civil Codification," No. 4 *Lawyer's World* (2003), at 4-5; Jing-Wei Liu, "Two Basic Problems Need to Be Settled in Civil Law Codification," in *Approaching to China to Cross Straight Private Law in the 21st Century* (2004), pp.125-146; Ping Jiang, "Adopting An Open Civil Code," No. 2 *Tribune of Political Science and Law* (2003), at 115-116); Ping Jiang, "Civil Law: Retrospective and Prospective," No. 2. *Journal of Comparative Law* (2006), p. 1.

With new leadership in 2013, the CCP adopted its Decision on Major Issues Concerning Comprehensively Deepening Reforms to initiate another compilation round for the Civil Code.[71] In 2014 the CCP explicitly linked the civil law codification process to its larger objectives of better protecting individual rights and safeguarding market development.[72] As a consequence, the Standing Committee of the NPC included civil law codification into its five-year legislative plan for 2013-2018, triggering a momentous push to solidify civil law principles, including those related to privacy and data protection.[73] While the first steps of the compilation process were completed in 2018, it took two additional years before the working committees within the drafting process could agree on the relative scope and reach of the provisions.

The Code divides privacy and data protection into separate provisions, with the rights and obligations differing depending on the context. As such, they reflect a hybrid regime like the European model in the sense that some of the definitions and the overreliance on consent demonstrate a focus on confidentiality and one's private life, while other definitions and processing obligations relate to fair information practice principles and exist independent of the right to privacy. In so doing, the Code converges nicely with other data protection regulations in China (including the PIPL), which relate to personal information processing, while also serving as a legal vehicle that uniquely emphasizes privacy in the normative sense.

While previous iterations of the Code contained provisions creating enforceable privacy rights, the newest compilation significantly expands those rights and creates a set of new obligations around personal data processing. Chapter Six defines privacy as a "natural person's peace of life and the private space, private activities and private information which she is unwilling to let others know" (Art. 1032) and lists activities that require consent from data subjects. Such activities include:

- Disturbing people's private lives through telephone, text message, instant messaging tools, email, and leaflets (Art. 1033),

[71] "Decision of the CCCPC on Some Major Issues Concerning Comprehensively Deepening the Reform" *The Supreme People's Court of the People's Republic of China* (2013), http://english.court.gov.cn/2015-10/08/content_22130532.htm
[72] CCP Decision 2014, https://www.chinalawtranslate.com/en/fourth-plenum-decision/
[73] "China Includes Civil Law Codification in Legislation Plan," *Global Times* (2015), https://www.globaltimes.cn/content/935674.shtml

- Entering, peeping, or recording other people's private space such as houses and hotel rooms (Art. 1033),
- Eavesdropping and publicizing other people's private activities (Art. 1033),
- Processing private information of other people (Art. 1033).

While violations of the right to privacy may result in civil liability, these provisions say little about data processing in the context of the platform economy. As we will see, this may indicate one reason why privacy litigation in China may not have that large of an impact on the regulation of platforms. Notwithstanding this, the Code outlines explicit provisions related to other data processing activities that share many similarities with other international data protection models.

For instance, the Code defines personal information (个人敏感信息) broadly as "all types of information recorded electronically or in other ways that can identify a specific natural person alone or in combination with other information" (Art. 1034).[74] A similar definition has been operationalized by other regulations around the world. Furthermore, personal information handlers (个人信息的处理者) must obtain consent from the data subject when collecting, storing, using, transmitting, providing, or publicizing personal data, unless another law or regulation provides otherwise.[75] They must also publicize the rules of processing, and express the purpose, method and scope of processing when obtaining consent.

Additionally, the Code notably sets forth data subject rights that align with the PIPL including the right to inquire about, copy, correct, and delete information held by an information handler. Broad exemptions exist for handlers that obtain consent, process information that is already public unless the data subject explicitly rejects the processing of the information or doing so would infringe upon her significant interests, and when reasonable to maintain a public interest such as public security or health.[76] Finally, the Code imposes information security obligations on information handlers. It specifically requires handlers to take technical and other necessary measures to ensure the security of the personal information it processes.[77] While the Code does

[74] The same definition is offered in the PIPL.
[75] Indeed, although heavily reliant on consent, the PIPL lists other lawful grounds for when data processing is appropriate. See Hunter Dorwart, Gabriela Zanfir-Fortuna & Clarisse Girot, "China's New Comprehensive Data Protection Law: Context, Stated Objectives, Key Provisions" *Future of Privacy Forum* (2021), https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/
[76] One notable example of this is the processing of personal data in response to the Covid-19 pandemic.
[77] Civil Code Art. 1038.

not explicitly reference any other law or regulation, these technical measures converge completely with notable provisions in China's emerging data security regulatory infrastructure.[78]

The broad convergence of the Civil Code and the PIPL with other data protection frameworks indicates that the central government envisions a role for courts to adjudicate individual claims on a smaller-scale basis. Indeed, as discussed below, cases based on the Code are increasing in both scale and frequency, and in certain circumstances have generated significant attention from regulators. However, the recent compilation of the Code should not be divorced from the larger issues and debates that have centered around the complicated development of private law in China. Legal reforms in this space have consistently faced institutional pressure stemming from the country's unique political and administrative structure, its embedded interests, and its practical constraints.[79] Leading up to the compilation process, many scholars disagreed about the path of codification, the degree to which the Code should represent a unified and holistic set of legal rights and obligations, and the relationship of the Code to other areas of commercial law.[80] It is important therefore not to overinflate the law's relevance as some watershed moment for judicial representation but still acknowledge that its current iteration represents an important step in solidifying legal process in the country.[81]

Where this process ultimately goes is the subject of much debate.[82] There is real pressure on the Chinese government to respond to the growing social harms of the platform economy and develop a functional civil legal system that suits China's particular needs and unique political structure.[83] Yet there are also real barriers facing legal reform generally (see below) and it is unclear to what extent individuals will use the judicial process, if at all, to enforce civil data privacy and protection expectations in the market economy and whether the exercise matters in the first

[78] Both the Cybersecurity Law and the Data Security Law outline relevant security protocols to follow with respect to the processing of both personal and non-personal data. In addition, a proliferation of data security standards developed in coordination with Technical Committee 260 (TC260) may provide further guidance.
[79] See Zhang *supra*, note 63.
[80] See Sun *supra*, note 69.
[81] Although the codification process was completed, leaders in China will certainly revisit some of the larger outstanding issues in the civil law process. Indeed, the recent "Plan on Building the Rule of Law in China (2020-2025)" to better develop China's "socialist rule of law with Chinese characteristics" suggests that the conversation around civil law codification in the country will enter a new "implementation" and "evaluation" phase shortly.
[82] Moritz Rudolf, "Xi Jingping Thought on the Rule of Law" *SWP* (2021), https://www.swp-berlin.org/10.18449/2021C28/.
[83] Huang & Shi *supra*, note 28.

place given the primacy of the larger centrally-coordinated bureaucracy in making regulatory decisions.

III. PRIVACY LITIGATION IN CHINA – TRENDS AND DATA[84]

Privacy litigation in China is increasing both in scale and frequency. While the Civil Code is not the only legal basis through which individuals bring these claims, its recent compilation has witnessed an uptick in cases in many provinces throughout China. As a generally applicable law across jurisdictions, the Civil Code applies broadly and creates enforceable rights and obligations on several natural and legal persons. Many cases recently litigated were initiated prior to the adoption of the Civil Code in 2020 and cite previous articles of law as causes of action. More recently, litigants have brought claims under the new provisions of the Code that deal specifically with personal information protection. Some of these cases have generated considerable media attention both within and outside of Chinese sources, including a now famous case in Hangzhou concerning the use of facial recognition technologies.[85] Nearly all the cases involve the prevalence of surveillance technologies or large databases of information. Finally, the introduction of a new system of prosecution, the civil public interest litigation system, may serve as one vehicle through which courts enforce privacy and data protection laws.

As discussed in the next section, an analysis of case law in China must recognize that while cases evidence a growing trend of platform regulation from the bottom up, they also mask that a huge majority of disputes are resolved through other mechanisms such as mediation or settlement.[86] Therefore, while the data suggests definitive and concrete trends, it inherently paints an incomplete picture. This will become critical for also contextualizing the role courts play in China vis-à-vis the central administrative system, a task necessary for any holistic approach to platform regulation. While privacy litigation is increasing, its significance in China's overall regulatory system may remain relatively underwhelming and stagnant, not the least because of the larger barriers in China's civil law system and its underlying legal culture.

[84] All of these cases were researched using China Judgments Online (中国裁判文书网), https://wenshu.court.gov.cn/
[85] Yuan Ye, "A Professor, a Zoo, and the Future of Facial Recognition in China" *Sixth Tone* (2021), https://www.sixthtone.com/news/1007300/a-professor%2C-a-zoo%2C-and-the-future-of-facial-recognition-in-china
[86] Sida Liu, "The Shape of Chinese Law," Vol. 1, No. 2 *Peking University Law Journal* (2014), pp. 415-444.

A. Cases Brought Under the Civil Code and other Civil Laws

Most of the noteworthy cases brought under the Civil Code involve smaller scale disputes between private citizens such as neighbors or family members and not conglomerated entities that collect and process large swathes personal information. They have primarily occurred in more developed jurisdictions in China and in circumstances where other avenues of conciliation were unsuccessful. While some litigants expressly reference Articles 1032-1039 of the Civil Code as the primary cause of action, many others center their claim around other theories such as breach of contract, tort, or violation of statutory law (e.g., consumer protection) and cite the Civil Code as evidence of the violation. As discussed above, there is a clear separation of privacy claims under the Civil Code (Art. 1032) from those related to data protection (Art. 1034-39). Recent cases do not suggest a pattern of outcome, as those identified demonstrate no asymmetrical favorability for either plaintiffs or defendants. However, plaintiffs have generally won more cases in two circumstances: 1) when they sue under the privacy provisions rather than those related to data protection; and 2) when they sue natural persons rather than corporate bodies or government offices. Courts have varied in their judgments and as a result, fact-specific particularities outweigh any general pattern in the data. In other words, while courts side with plaintiffs in certain circumstances over others, the *reasons* for doing so vary with the facts and do not justify any empirical generalization.

In judgments held for the plaintiff, defendants either obtained or disclosed personal information covered by the law without the plaintiff's clear consent. For instance, one early case in Guangdong province held that setting up a surveillance camera towards a neighbor's door was a clear violation of Article 1032, while another in Sichuan found that disclosing a customer's address, contact number and WeChat name on a social media forum violated Article 1034's relevant data protection provision.[87] Both cases involve a private dispute between two *individual natural persons* and are straightforward in the facts insofar as the circumstances fall nicely within the statutory text of the Civil Code.[88] Other cases examined exhibited a similar tendency of

[87] 丁伟洪雅县云洁干洗店一审民事判决书(2021)川 1423 民初 38 号; 谭永森与谭锦林隐私权纠纷一案民事一审判决书（2020）粤 0605 民初 29988 号

[88] Setting up a camera is a textual violation of the law while disclosing private information gained during a business transaction falls nicely within the personal information processing obligations.

outcome. Indeed, the author could find no cases where the defendant won as a private individual, unassociated with a company or other business entity.

By contrast, plaintiffs were more likely to lose when suing a private company or public office—something not too dissimilar from the U.S. experience. Under Article 1032 privacy provisions, courts in China have dismissed cases when the information gathered was previously made public to a third-party. For instance, in Shandong province, a man unsuccessfully sued his boss for obtaining his home address through the man's job application and subsequently acting upon that information by visiting him at home.[89] Another case in Guangdong found that a mobile app did not violate the plaintiff's privacy rights when it disclosed a maintenance record of used cars because the company legally collected the information.[90]

With respect to claims brought under the data protection provisions, a similar trend is noticeable. In the same case in Guangdong, the court also dismissed claims under Art. 1034 because the company properly de-identified the data prior to disclosure.[91] In Chongqing, a plaintiff tried to bring a case against a credit lending platform after the platform disclosed the plaintiff's information to a government credit reporting entity when he defaulted on the loan.[92] The plaintiff argued that the credit reports harmed him by making it more difficult to get a mortgage in violation of Article 1036 of the Civil Code. The court dismissed the case, reasoning that the platform took reasonable steps to verify the information, ensured that it was not disclosed to other people, and therefore did not harm the plaintiff sufficient to violate the law.

Additionally, courts have been even more reluctant to side with plaintiffs against public bodies. In one case, an individual requested information about another from a local civil affairs bureau, arguing that the law gave him the right to request information "related to government affairs."[93] The court disagreed and cited Article 1039 of the Civil Code to justify its claim that the law required government offices to protect personal information if disclosure of such information would have harmful effects on the data subject. Here, the information concerned a recent divorcee—any disclosure of that information would have negative repercussions in the community

[89] 张磊与谢强隐私权纠纷二审(2021)鲁 01 民终 579 号民事判决书 （2021）鲁 01 民终 579 号
[90] 余某与北京酷车易美网络科技有限公司隐私权纠纷一审民事判决书
[91] Ibid.
[92] 潘洪霞与北京捷越联合金融信息服务有限公司中国人民银行征信中心侵权责任纠纷一审民事判决书 （2021）渝 0104 民初 778 号
[93] 徐宏强与玉环市民政局、玉环市人民政府行政监察(监察)一审行政判决书 （2021） 浙 1021 行初 10 号

as understood in the Chinese cultural context. In another notable case, a man requested information from the Beijing Yanqing District Jingzhuang Town Government and then sued the municipal body when it published a statement in its disclosure that the plaintiff specifically requested the disclosure.[94] The court held for the defendant and reasoned that releasing the name of the person who requested the information promotes transparency of government and therefore is pertinent to public welfare (an exception under the Civil Code).

Nonetheless, plaintiffs have won cases brought against larger corporate bodies or public organizations. In one case, an employer terminated an employee's contract for missing work without providing proof of medical conditions as per the company's policy.[95] The plaintiff employee had in fact sent relevant materials to the employer, but not to the level of specificity the company demanded. The court ruled in favor of the plaintiff, finding that Article 1034 protected the details of a medical condition when the company only required proof of the medical condition itself.

Perhaps the most famous privacy case so far in China, an attorney in Hangzhou brought a case against a zoo after they required him to agree to their use of facial recognition technology to monitor people accessing the zoo through an annual pass that previously required obtaining customers fingerprints.[96] Notably, the plaintiff brought claims under multiple sources of law, including the Consumer Protection Law and breach of contract. The court dismissed his claim under the Consumer Protection Law, reasoning that the zoo was transparent about its requirements for purchasing the annual pass but sided with the plaintiff under a theory of breach of contract. Specifically, the court held that by unilaterally modifying its terms of contract to include new provisions on collecting facial recognition information, it violated the law. Plaintiff did not agree with nor negotiate against the additional terms and the new requirements, and the zoo, while not restricting the ability of the plaintiff to use the pass, nevertheless increased his burden under the new requirements. The attorney in this case not only collected a total refund of the annual pass but also persuaded the court to require the zoo to delete his biometric information.

He did not, however, stop the zoo or other similar entities from using facial recognition altogether. This has now become his public goal and he is currently appealing his case to a higher

[94] 枢琦与北京市延庆区人民政府等其他二审行政判决书 （2021）京 01 行终 44 号
[95] 达科信息科技（北京）有限公司与谢涛劳动争议二审民事判决书 （2021） 京 03 民终 106 号
[96] 兵与杭州野生动物世界有限公司服务合同纠纷一审民事判决书 (2019）浙 0111 民初 6971 号

judicial body.[97] The case generated noticeable attention both inside and outside of China because it not only demonstrated public backlash against facial recognition technology generally but also the successful use of the court system in China to combat its use.[98] While awaiting appeal, the SPC released regulations clarifying its interpretation of the law with respect to facial recognition.[99] These regulations notably reference other laws in China's emerging ecosystem such as the PIPL and the Civil Code and may have a direct impact on the future proceeding of this case and others.

B. Civil Public Interest Litigation

One unique form of judicial enforcement of privacy and data protection provisions concerns the civil public interest litigation system, a relatively new process where prosecutors bring civil cases against larger defendants on behalf of the public interest.[100] Cases of this nature usually involve very sensitive activities of private actors that risk harm to a great number of individuals. For instance, prosecutors have brought cases under the civil public interest mechanism to enforce environmental and consumer rights laws.[101] As discussed below more thoroughly, this enforcement system should be seen as complementary to the larger top-down central administrative process and used in circumstances to enforce the laws against companies evade enforcement action from ministerial bodies.

The civil public interest litigation system may soon focus more on data protection and privacy generally. In June 2020, the China's Supreme People's Procuratorate stated it would expand the scope of these lawsuits to digital rights, including the rights of minors online.[102] Since then, prosecutors across China have brought cases that directly implicate privacy and personal information protection. Up until 2021, these cases mostly involved intervening against actors that

[97] See Ye *supra*, note 86.
[98] Xinmei Shen, "China's First Facial-Recognition Lawsuit Comes to an End with New Ruling and New Questions About the Fate of Individuals' Data" *South China Morning Post* (2021), https://www.scmp.com/tech/policy/article/3129226/chinas-first-facial-recognition-lawsuit-comes-end-new-ruling-and-new
[99] Supreme People's Court Guidelines on the Use of Facial Recognition Technology. http://www.court.gov.cn/fabu-xiangqing-315851.html
[100] 最高人民法院关于审理消费民事公益诉讼案件适用法律若干问题的解释
[101] "Public Interest Litigation in China" *Yale Law School: Paul Tsai China Center* (2021) https://law.yale.edu/china-center/resources/public-interest-litigation-china
[102] "Work Report of the Supreme People's Procuratorate" *Xinhua* (2020), https://www.spp.gov.cn/spp/gzbg/202006/t20200601_463798.shtml

took advantage of big platforms' cybersecurity vulnerabilities and not against the platforms themselves. For instance, in Shanghai, prosecutors brought a case against an employee of Zhongtong (one of the biggest delivery companies in China) who gathered and sold personal information of shipping orders by abusing his position within the company.[103] In addition, another litigation witnessed a group of individuals in Jiangsu face liability for abusing Baidu's password recovery process to gain unauthorized access into users' accounts and then sell that information on a black market.[104]

However, recent data suggests that civil public interest lawsuits may soon target larger platforms for violating privacy and data protection regulations. In August 2021, prosecutors in Beijing initiated a lawsuit against WeChat on the grounds that the company was violating China's child protection laws with its service.[105] Likewise, Kuaishou recently settled a public interest lawsuit in Hangzhou specifically over its violation of child protection laws when it collected information of minors without notifying their parents or guardians.[106] Both companies have offered specialized services and product offerings to minors for years and often in ways that raised eyebrows in Beijing's larger regulatory circles.[107] The introduction of the civil public interest litigation system in this context could increase regulatory pressures on platforms and may serve as one vehicle through which courts directly enforce privacy and data protection laws.

Table 2: Outline of Recent Data Privacy Cases in China

Name	**Source of Law**	**Major Issue**	**Date**
谭永森与谭锦林隐私权纠纷一案民事一审判决书 (粤 0605 民初 29988 号)	Civil Code (Art. 1032) 中华人民共和国民法典第一千零三十二条	Setting up a surveillance camera towards a neighbor's door.	2020

[103] 暨原审附带民事公益诉讼被告人王耀杰侵犯公民个人信息二审刑事裁定书（2021）沪 02 刑终 245 号
[104] 刘某侵犯公民个人信息二审刑事裁定书（2020）苏 02 刑终 333 号
[105] "Announcement of the People's Procuratorate of Haidian District of Beijing on the Initiation of a Civil Public Interest Lawsuit Against Shenzhen Tencent Computer System Co., Ltd." *Justice Net* (2021), http://www.jcrb.com/xztpd/gxzt/sqgg/202108/t20210806_2306228.html
[106] Iris Deng, "Beijing's Prosecutor's Public Interest Lawsuit Against Tencnt Raises New Concerns for China's Big Tech Sector" *South China Morning Post* (2021), https://www.scmp.com/tech/big-tech/article/3144426/beijing-prosecutors-public-interest-lawsuit-against-tencent-raises
[107] "Report of the Constitution and Law Committee of the National People's Congress on the Deliberation Results of the "Personal Information Protection Law of the People's Republic of China (Draft)" *National People's Congress* (2021), http://www.npc.gov.cn/npc/c30834/202108/a528d76d41c44f33980eaffe0e329ffe.shtml

枢琦与北京市延庆区人民政府等其他二审行政判决书 (京 01 行终 44 号)	Civil Code (Art. 1032) 中华人民共和国民法典 第一千零三十二条	Disclosure of a DSAR against a town government.	2021
张磊与谢强隐私权纠纷二审 (鲁 01 民终 579 号民事判决书)	Civil Code (Art. 1032) 中华人民共和国民法典 第一千零三十二条	Unauthorized disclosure of employment data from employer.	2021
丁伟洪雅县云洁干洗店一审民事判决书 (川 1423 民初 38 号)	Civil Code (Art. 1032-34) 中华人民共和国民法典 第一千零三十二条	Business disclosed customers' private information online.	2021
余某与北京酷车易美网络科技有限公司隐私权纠纷一审民事判决书 (粤 0192 民初 928)	Civil Code (Art. 1032-34) 中华人民共和国民法典 第一千零三十二条	App provided personal information connected to the sale of used cars.	2021
兵与杭州野生动物世界有限公司服务合同纠纷一审民事判决书 (浙 0111 民初 6971 号)	Consumer Protection Law (中华人民共和国消费者权益保护法)	Zoo in Hangzhou suddenly required patrons to register facial information.	2019
达科信息科技有限公司与谢涛劳动争议二审民事判决书(京 03 民终 106 号)	Civil Code (Art. 1032-34) 中华人民共和国民法典 第一千零三十四条	Employer demanded employee disclose sensitive medical data	2021
潘洪霞与北京捷越联合金融信息服务有限公司中国人民银行征信中心侵权责任纠纷一审民事判决书 (渝 0104 民初 778 号)	Civil Code (Art. 1036) 中华人民共和国民法典 第一千零三十六条	Loan service platform disclosed the customer's default on loan to government credit offices.	2021
徐宏强与玉还市民政局，玉环市人民政府行政监察(监察)一审行政判决书（浙 1021 行初 10 号）	Civil Code (Art. 1036) 中华人民共和国民法典 第一千零三十九条	Plaintiff sues government office for not disclosing information of a recent divorcee.	2021
余×非法获取公民个人信息罪二审刑事裁定书 (二中刑终字第 995 号)	Criminal Code (Art. 253) 《刑法》第二百五十三条	Illegal purchasing of PI over the Internet.	2014
张亚军、周志刚出售、非法提供公民个人信息罪二审刑事裁定书 (浙 07 刑终 1183 号)	Criminal Code (Art. 253) 《刑法》第二百五十三条	Illegal selling of PI (phone numbers and names) online.	2018
箫锴泉侵犯公民个人信息罪一审刑事判决书 (桂 0405 刑初 206 号)	Criminal Code (Art. 253) 《刑法》第二百五十三条	Illegal selling of WeChat and QQ accounts for profit.	2019

邓长久、张国芳等出售、非法提供公民个人信息罪二审刑事裁定书（琼 97 刑终 297 号)	Criminal Code (Art. 253) 《刑法》第二百五十三条	Spam calling regarding changes to airline tickets.	2018
李骏杰犯破坏计算机信息系统罪胡某犯出售、非法提供公民个人信息罪董某、黄某等犯非法获取公民个人信息罪二审刑事裁定书(浙杭刑终字第 311 号)	Criminal Code (Art. 253) 《刑法》第二百五十三条	Hacking and sabotaging computer systems and public records.	2015
暨原审附带民事公益诉讼被告人王耀杰侵犯公民个人信息二审刑事裁定书(沪 02 刑终 245 号)	Civil Public Interest Litigation	An employee of a large delivery company collected and sold personal information of customers.	2021
刘某侵犯公民个人信息二审刑事裁定书 (苏 02 刑终 333 号)	Civil Public Interest Litigation	Defendant abused Baidu password recovery system to gain unauthorized access to accounts.	2020

IV. THE ROLE OF COURTS – COMPLEMENTARY OR INSIGNIFICANT

While these recent cases suggest that the court system could play a role in regulating the platform economy, it is important to contextualize this role with the larger administrative and regulatory system to avoid drawing improper conclusions. Because of China's unique administrative system, privacy and data protection litigation should be seen as a secondary yet complementary mechanism of platform regulation. In other words, courts will likely intervene against big dominant platforms and other tech companies as a *stop-gap* measure in cases where regulation from the ministerial and super-ministerial levels fall short. They will not be the source of an independent lever of governance power in the platform economy nor will they drastically alter the internal compliance analysis of the biggest tech companies.[108] Despite this, courts will likely play a smaller role in resolving disputes that fall outside of the ambit of the central regulators and may even complement the larger regulatory system with civil public interest lawsuits.

Although all regulatory agencies in China are subordinated under the State Council, their competences often overlap in ways that produce regulatory ambiguity. Such ambiguity has proven

[108] See e.g., Randall Peerenboom, *China's Long March Toward Rule of Law* (2002), Kenneth Lieberthal, *Governing China* (1995).

an effective cornerstone of developing compliance culture in China's private sector as any company may be subject to oversight from multiple regulatory authorities under the same law or regulation. For instance, many of the key regulations in China's emerging data protection ecosystem were drafted in coordination with multiple agencies including the State Administration for Market Regulation (SAMR), the Ministry of Industry and Information Technology (MIIT), the Ministry for Public Security (MPS), the Ministry for State Security (MSS), and the Ministry of Transport (MOT). Additionally, the CAC, which serves as the primary Internet regulator, operates as a super-ministerial coordination and consultation body, and has its own prerogatives for developing regulations and technical standards in this space that in many respects supersede the agencies on the ministerial level.

Due to the complexity of this system, Chinese authorities will administer platform regulation largely from the top-down and not the bottom-up. This complements the country's deep-rooted historical practice, summarized in the phrase "three positions, one unity" (三位一体), that places great emphasis on the differentiation of legal compliance between multiple administrative institutions.[109] The prevalence of this large coordination and enforcement system in regulating the platform economy also reinforces the expectation that the political structure will continue to predominately guide the development of commercial and private affairs in China. While this does not mean there is no role for courts and individuals in this system, these institutional mechanisms primarily operate as a warning for other market participants to comply with the expectations of the central authorities—a process of "killing the chicken to scare the monkey" (杀鸡儆猴).

The relationship of the courts to the larger administration system also complements longstanding debates about the codification of civil law and the penetration of the Chinese legal system into commercial and private affairs. Indeed, while Chinese courts have witnessed an uptick in cases brought under the updated personality rights and data protection provisions in the recently compiled Code, such data ignores the widespread institutional presence of other forms of dispute resolution such as mediation through People's Mediation Committees or other forms of extra-judicial settlement.[110]

This complicates a strict analysis of data protection through China's court system for many reasons. First, because civil law has always been relatively underdeveloped in China,

[109] See Liu *supra*, note 87.
[110] Ibid.

especially when compared to criminal law, the transition to a "socialist market economy" in the 1980s brought with it many challenges to facilitate commercial and private matters.[111] The completion of the Civil Code may evidence resolution of some of those challenges but leaves others unaddressed. For instance, although the updated personality rights give individuals an ability to enforce privacy and data protection standards vis-à-vis other "private" actors, they do little to differentiate between private natural persons and private legal persons in the form of companies or other related legal constructions. This leaves much room for the central administration to continue to exercise great influence in the overall direction of regulation in the country.

Second, the use of legal categories commonly found in the EU and the United States such as "private/public" and "citizen/government" does not readily apply in the Chinese context and any attempts to reduce them to explain developments in Chinese law should not ignore the issue.[112] Indeed, the Chinese legal system must be understood through analytical frameworks attached to its own historical practice—including the use of conventional terms and conceptual schema to describe the functioning of government and the differential power-sharing relationships within it.[113] Historical experience suggests that law serves as an instrument to effectuate other social and moral goals and operates underneath the purview of the state administrative complex. This does not mean that the operationalization of law in China has been stagnant or consistent over time. On the contrary, China's legal system has reflected the country's recent history—it has evolved to accommodate the country's rapid growth in the past four decades but has in other respects retained its unique Chinese characteristics. China's legal system, like many other aspects of the country, is likewise undergoing a new phase of transformation and demands a reevaluation of the conceptual schema used to describe it.

Third and relatedly, despite these conceptual issues, data protection case law in China has so far focused solely on the "private-to-private" or "private-to-government" relationship and not the "private-to-company" relationship that many within China highlight as the primary source of platform-related harms. Trends do not indicate that individuals will pursue claims against private

[111] See Zhang *supra*, note 63.
[112] Donald C. Clarke, "Methodologies for Research in Chinese Law" Vol. 30, *University of British Columbia Law Review* (1996), pp. 201-209.
[113] Donald C. Clarke, "Regulation and Its Discontents: Understanding Economic Law in China." Vol. 28 *Stanford Journal of International Law* (1992).

companies in the same way they would in other legal systems such as the United States. Nor does the structure and function of China's legal system suggest that the law should be operationalized to do so. However, recent suits brought under the civil public interest litigation system may indicate a trend towards a more active court system in China, albeit one that directly aligns with the overall regulatory objectives of the central level.

Fourth, in some circumstances, the Chinese government struggles to implement national laws evenly and effectively on the local levels. The same may be true of China's data protection arsenal—including the PIPL. Indeed, many commentators have highlighted how the party cadre appointment process coupled with relative decentralized power-sharing arrangements creates incentives for local government officials to selectively implement the laws, which has led to problems of effective governance management from the top.[114] Courts are uniquely situated to ensure that laws passed in Beijing are enforced on the ground, but for a variety of reasons struggle to execute their orders.[115] Like other civil matters, with respect to data protection, courts may provide one mechanism for the center to ensure that obligations and rights contained in the law are followed on the ground. Without meaningful enforcement on the local level, the data protection provisions concerning data subject rights may fall short of their goals and become ineffective mechanisms for addressing social harm in the online world. This ability to funnel power from the top may see the role of courts enhanced in the future, especially if regulators in Beijing find it difficult to target data processing practices outside of the major industrial and urban centers.

V. CONCLUSION

[114] See e.g., Rogier Creemers & Susan Trevaskes, "Ideology and Organization in Chinese Law: Towards A New Paradigm for Legality" *Law and the Party in China* (2021); Neysun Mahboubi, "The Future of China's Legal System" *Chinafile* (2016); Benjamin Van Rooji et al., "Pollution Enforcement in China: Understanding National and Regional Variation" *Routledge Handbook of Environmental Policy in China* (2017); Zhao Yanrong, "The Courts' Active Role in the Striving for Judicial Independence in China" *Frontiers L. China* (2017); Kenneth Lieberthal, *Governing China* (1994).

[115] Local governments in some instances have more power than courts, which creates effective legal governance problems when a defendant is associated with the head of the local government or someone influential in the local party committee. Courts may issue orders declaring that an individual or corporation violated the law but without stronger authority cannot force that individual or corporation to comply with the judgment. While overtime this problem has been addressed at the central level, notably with the 14th Plenum's Decision Concerning Some Major Questions in Comprehensively Moving Governing the Country According to the Law Forward, the incentive structures have not changed much. See Donald C. Clarke, "Power and Politics in the Chinese Court System: The Enforcement of Civil Judgments" *Columbia Journal of Asian Law* Vol. 10, No. 1 (1996).

In China, the recent adoption of the PIPL and the Civil Code has introduced a new set of data subject rights directly related to data protection. While many of the provisions dealing with privacy predate the most recent iteration of the Code, the latter's completion significantly inscribes these civil principles into China's larger legal system and give individuals the ability to bring forth claims against other private actors. Such rights are reinforced by the PIPL, China's first comprehensive and nationally applicable data protection law, which sets forth similar terminology, processing obligations, and legal frameworks seen in the GDPR.

Individuals in the country have and continue to bring more privacy and security claims against individuals and companies under various laws, including the newly compiled Civil Code. Such litigation is increasing both in frequency and scope in China, although litigants mostly pursue claims against smaller-scale actors and not major platforms or large-scale public bodies. This is in conformity with expectations of how China's legal system operates, as judicial institutions have historically not been the source of social change in the country. However, the relatively new civil public interest litigation system may witness more cases brought against larger platforms that directly alter corporate behavior in line with actions taken on the ministerial level.

The nature of the Chinese judicial system makes such litigation less important in the overall regulatory scheme. Rather, the central government will continue to drive regulatory decision-making with respect to the activities of large online platforms. Nonetheless, privacy litigation may help individuals and organizations address harms caused by smaller and less visible businesses and even shed further light on how companies should comply with the myriad sectoral regulations passed by various competent authorities. Litigation in China thus complements the vast apparatus of ministries centralized under the State Council and their goals regarding the platform economy but in a secondary and limited way. Further legal developments in China could complicate this image and resonate broadly with debates regarding the penetration of Chinese law into civil and private matters.