Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Mapping the development of China's data protection law: Major actors, core values, and shifting power relations ☆

Bo Zhao [a], *Yang Feng* [b,*]

[a] *Tilburg Institute of Law, Technology, and Society, Tilburg University, the Netherlands*
[b] *Guanghua Law School, Zhejiang University, China*

A B S T R A C T

This Article seeks to map the possible paths of the development of China's data protection law by examining the changing power relations among three major actors - the State, digital enterprises and the public in the context of China's booming data-driven economy. We argue that focusing on different core values, these three major actors are the key driving forces shaping China's data protection regime. Their dynamic and multidimensional power relations have been casting the development of China's data protection law with various uncertainties. When persuing different, yet not always conflicting values, these three major actors may both cooperate and compete with each other. Based on our careful analysis of the shifting power relations, we identify and assess three possible paths of the development of China's data protection law. We are much concerned that the proposed comprehensive data protection law might be a new attempt of the State to win legitimacy abroad, while actually trying to reinforce massive surveillance besides economic goals. We argue that a modest alternative may be that this law might show some genuine efforts for protecting data privacy, but still with poor enforcement. Last, we argue that the most desirable development would be that this law could provide basic but meaningful and effective protection for data privacy, and lay a good foundation for further development.

1. Introduction

On April 10 and April 11, 2018, Mark Zuckerberg testified before the U.S. Congress. He argued that strictly regulating U.S companies' use of personal data would cause U.S. companies to fall behind Chinese companies when it comes to data-intensive innovation like artificial intelligence.[1] His concern is that Chinese companies are not constrained by stringent data protection regulation and will gain an edge.[2] Zuckerberg's argument partially reveals that China's weak personal data protection has allowed Chinese digital giants to achieve spectacular developments in past years. However, his argument is rather stereotyped, overlooking the complexity of the multi-layered development of China's data protection law, and thus largely overlooking the considerable progress of China's data protection law.

As a rising data power, China has been infamous for her weak personal data protection both in law and in practice, first because of the State's broad access to corporate data, and second because of the rampant data breaches and privacy invasions across the country.[3] The development of China's data

☆ This research was financially supported by National Office for Philosophy and Social Science (Grant Number 18CFX027) and 2019 Special Project on Artificial Intelligence and Law of Guanghua School of Law, Zhejiang University.

* Corresponding author: Yang Feng, Guanghua Law School, Zhejiang University, China.
E-mail address: feng_yang@zju.edu.cn (Y. Feng).

[1] Samm Sacks and Lorand Laskai, 'China's privacy conundrum', Slate Magazine, 2019 <https://slate.com/technology/2019/02/china-consumer-data-protection-privacy-surveillance.html> Accessed 20 July 2020.

[2] ibid.

[3] Paul de Hert and Vagelis Papakonstantinou, 'The data protection regime in China', the Committee on Civil Liberties, Justice and Home Affairs of European Parliament, 2015, pp. 24-27. <https://works.bepress.com/vagelis-papakonstantinou/37/> Accessed 20 July 2020.

https://doi.org/10.1016/j.clsr.2020.105498
0267-3649/

protection law has drawn increasing attentions of Chinese legal scholars. But the majority of the existing research focuses on classic legal analysis of specific development of the data protection legal framework, per se, failing to provide a systematic and in-depth reflection of the underlying political-legal logics that are decisive in shaping the legal framework.[4] Western scholars and practitioners oftentimes fall short of having a up-to-date observation on the development of China's data protection law. Both domestic and foreign observers are unable to catch up with many positive law developments collectively driven by the State, digital enterprises, ordinary Chinese people, and foreign forces.[5] There have been lacking comprehensive studies to address the shifting power relations and power dynamics among the above-mentioned major actors, where they collaborate and confront with each other under different circumstances.

In this Article, we aim to assess the development of China's data protection law in a systematic way, by exploring the dynamic power relations between three major actors who are dominating the policy/law-making arena of data protection in China. These three major actors include the State, digital enterprises, and the public. This Article is structured as follows. Following the introduction, the second section discusses the three major actors and their influences on China's data protection legislation. The third section illustrates the significance of the three core values of these major actors. This section argues that the future development of China's data protection law lies largely in the constantly shifting interactions of the three core fundamental values - public security, economic growth and data privacy protection – as well as the gravity that the different actors put on them. The fourth section assesses three possible paths of the development of China's future data protection law. The fifth section is the conclusion.

2. Preliminaries: power relation and major actors

Identifying major actors and their power relations in specific socioeconomic context is essential to understand the course of the legal development of data protection in China. It is thus necessary to examine the crucial interests and values of these actors. For this purpose, this section first introduces the concept of power relations as the analytical framework.[6] Power relations can be approached from three dimensions. First, as Robert A. Dahl put it, "A has the power over B to the extent that A can get B to do something that B would not otherwise do."[7] Second, A can exercise power *indirectly and passively* to exclude issues of the relevance to B, like by agenda setting according to Bachrach and Baratz. Third, following Luke, the power relation can be created by conducting "the socially structured and culturally patterned behavior of groups and practices of institutions," or by exercising the "non-decision-making power". These three dimensions of the power relations can well capture and explain the shifted and still shifting power dynamics in the development of China's data protection law between the State, digital enterprises, and the public.

The Chinese government is undeniably the most important actor in data protection area given its political dominance in an authoritarian state.[8] China is a unitary country. Despite continuous decentralization of power to lower-level units, the Chinese central government has been the principal driving force in promoting policy and law developoments, not only possessing the main decision-making power, but also controlling the pace of policy/law implementation.[9] In terms of power relation, the State enjoys the dominating status over other actors in law development and is able to implement its own wills unilaterally.

The State's dominating power is observable from three dimensions: ordering other actors to do things, influencing other actors indirectly or passively, and creating socially and culturally patterned behavior. One such apparent example in the economic domain is the State's direct control of State-owned enterprises (hereafter SOEs) especially in industrial sectors that have been identified as key to China's national security and economic development.[10] But for the rule of law reason, the State has become rather cautious to use direct, coercive force to implement its intentions, although this may still happen in extreme cases (such as suppressing collective resistance and political dissidence, which are deemed as a direct threat to the government ruling).[11] Consistent with technological advances that continuously provide new technological tools for use, the Chinese state becomes more powerful and efficient in setting and implementing its political agenda

[4] A few existing research has lightly touched upon the paths of China's data protection law, see Fuping Gao, 'Personal information protection: from individual control to social control' (个人信息保护:从个人控制到社会控制) (2018) Chin J Law (《法学研究》), pp. 84–101; Hanhua Zhou, 'Exploring the personal data governance that achieve incentive compatibility — China's personal information protection' (探索激励兼容的个人数据治理之道 — 中国个人信息保护) (2018) Chin J Law (《法学研究》) , pp. 3–23.

[5] For instance, in his 2012 article about the global data privacy law development, Graham Greenleaf briefly discussed the prospects of China's data protection law, see Graham Greenleaf, 'The influence of European data privacy standards outside Europe: implications for globalization of convention 108', *Int Data Priv law* 2 (2012), p. 70

[6] The use of power relation as this paper's analytical framework is inspired by Prof. Bert-Jaap Koops' analysis of the shifting power relations in law and technology development, See: Bert-Jaap Koops, 'Law, technology, and shifting power relations', *Berkeley Technol Law J* 25 (2010).

[7] Robert A. Dahl, 'The Concept of Power', *Behav Sci* 2 (1957), pp. 201-215.

[8] For the Party domination of the State, see: Yongnian Zheng, *The Chinese Communist Party as organizational emperor: culture, reproduction, and transformation* (Routledge, Oxon, 2010), pp. 98-108.

[9] Utill today the judiciary and the legislation are under the firm control of the Chinese Communist Party due to the lack of separation of powers. See: Michael R. Pompeo, 2018 Country reports on human rights practices: China, U.S. Department of State, 2019, <https://www.state.gov/wp-content/uploads/2019/03/CHINA-INCLUDES-TIBET-HONG-KONG-AND-MACAU-2018.pdf> accessed 20 July 2020.

[10] Deborah Healey, 'Mergers with Conditions in China', in Lisa Toohey, Colin B. Picker and Jonathan Greenacre (Eds.), *China in the international economic order: new directions and changing paradigms* (Cambridge University Press, New York, 2015), pp. 245-267.

[11] Yongshun Cai, *Collective resistance in China: why popular protests succeed or fail* (Stanford University Press, California, 2010), pp. 1-3.

as well as defending its core values.[12] This is much obvious in the use of facial recognition technologies for improving public security and law enforcement purposes in a number of Chinese cities.[13] Using industrial policy and strategy to influence the private sector has in recent decades become an apparent trend in the context of national economic planning, such as the famous "Made in China 2025", as will be further discussed in this paper. Last, the Chinese state has dominating influence on Chinese corporate cultures in multiple forms, including privately owned or managed corporations.[14]

The second major actor in the development of data protection law in China is digital enterprises. Apart from spectacular expansion of traditional industries such as automobile, shipbuilding and electricity, the emerging digital industries driven by private entrepreneurship and innovation have been one of the most important elements of China's economic development in the past decades. Consistent with China's fast tech-economic development, the economic and political power of private digital giants has been rising. Among a number of digital giants, the most noticeable are Huawei, Alibaba, Tencent, and Baidu. At the subnational level, private digital companies have been increasingly influential via providing goods/services as well as job opportunities to millions of Chinese citizens. At the national level, these enterprises have become very proactive in promoting the policy and legal movements - they have become important actors in industrial standards setting and policy making, as well as in other political activities such as attending diplomatic trips with Chinese ranking officials.

Given their sheer economic influence, these digital enterprises have become increasingly assertive and dare to publicly challenge the central government's decisions when these decisions infringe upon their core interests. In 2015, when the State Administration for Industry and Commerce (SAIC) issued a report, criticizing the rampant sale of counterfeit goods on Alibaba's E-commerce platform, Alibaba immediately fought back and almost won the battle against the SAIC.[15] Normally Chinese enterprises would not dare to publicly criticize the government, they instead tend to solve disputes via negotiations and other informal means. The 2015 Alibaba's unusual public defense has at least two implications. First, it suggests the increasing capacity of private digital giants, by transferring economic and technology capacities into soft power, to (re)shape their relations with the State. Second, it shows that Chinese digital giants have built complex relationships with the government. They oftentimes team with the government to push for common objectives (such as formulating more tolerable economic policies), but they sometimes choose to stay away or even oppose unfavorable government decisions.

The third major force in the development of Chinese data protection law is the public, which is the weakest actor among the three due to China's authoritative political apparatus and nascent development of civil society. Nevertheless, in parallel with the rapid increase in the population of Netizens and their awareness of rights protection, the recent years have seen the continuous increase of the public's voice in data protection lawmaking. Such development has led to more exposure of data security accidents, to more transparency in data processing on both government and corporate sides, to more active participation in law/policy-making processes, and to more reputation consideration both of the State and digital enterprises.[16]

Data privacy has become a serious concern of the Chinese public, but not always so, especially when economic interests and convenience are involved. In addressing a business conference, Robin Li, the founder and CEO of Baidu, stated: "Chinese are insensitive to private issues and in most occasions, they are willing to gain convenience at the expense of privacy".[17] Li's statement immediately triggered wide criticism. Nevertheless, his statement reveals certain truth – for the Chinese public, privacy seems to be a tradable value, and Chinese digital giants are very good at taking advantage of such trade-off by providing increasingly user-friendly digital goods and services. The public may stand with the State against aggressive corporate misuse/abuse of their personal data in a number of occasions, but they may also support digital enterprises against government's unlimited access to their personal data. Generally speaking, the public is relatively powerless in influencing the setting of the legislative agenda, except for a few scholars and opinion leaders who would speak out on behalf of the public, and can pose some pressure for policy/law makers.

Apart from the three major actors, various foreign forces serve as another important factor that has been influential in

[12] The legislation about Internet filtering shows that Chinese government is not hesitant to embrace new information technology for law enforcement purposes, see: Jyh-An Lee and Ching-Yi Liu, 'Forbidden city enclosed by the great firewall: the law and power of Internet filtering in China', Minn J Law, 13.1(2012) Sci Technol, pp. 125-126.

[13] Paul Mozur and Keith Bradsher, 'China's A.L. advances help its tech industry, and state security', the New York Times, 3 December 2017.

[14] Colin Hawes' in-depth analysis of Chinese corporate culture rightly reveals that the Chinese state, in particular, the Chinese Communist Party (hereafter the CCP) has to a large extent successfully created a prevailing (official) corporate culture among both SOEs and private-owned enterprises. The creation of such culture is achieved via multiple means, including the strong involvement of CCP in corporate governance, as explicitly expressed in government and Party documents and in the Company Law, with CCP's "leading role" in economy revived and the Chinese socialist and traditional communitarian culture retained, See: Colin Hawes, 'The Chinese transformation of corporate culture' (Routledge, Oxon, 2012), pp. 129-136, also see Colin Hawes, Representing corporate culture in china: official, academic and corporate perspectives, *China J* 59(2008), pp. 33-40.

[15] See: Charles Clover, Alibaba slams watchdog's 'unfair' report, FT, 2015, < http://www.ftchinese.com/story/001060413/en?archive> Accessed 20 July 2020.

[16] 《中国数字经济发展白皮书》 (White paper on the development of china's digital economy), China Academy of Information and Communications Technology, 2020, <http://www.caict.ac.cn/kxyj/qwfb/bps/202007/t20200702_285535.htm> Accessed 25 July 2020.

[17] See 谈及隐私惹众怒, 李彦宏哪里说错了 (The Privacy Talk triggered wide criticism, what is wrong about Robin Li), 中国青年报(China Youth Daily), 2018, <http://zqb.cyol.com/html/2018-03/28/nw.D110000zgqnb_20180328_5-02.htm> Accessed 20 July 2020.

the development of China's data protection law. Such foreign forces can be large foreign corporations that have considerable economic interests in China, foreign governments that have continuously criticized China's low level of data privacy protection, and foreign NGOs and scholars that have been monitoring the development of China's data protection law. The U.S government, for example, has frequently accused China of having established a regulatory regime that requires and pressures the transfer of cutting-edge technology from U.S. companies to Chinese entities.[18] The forced technology transfer not only enables Chinese entities to systematically obtain intellectual property, but also enhances Chinese government's ability to access ordinary citizens' personal data. These foreign forces are not decisive in the first and second dimensions of power relations, although they might be involved in creating the global legal and cultural environment that may influence China's data protection law to some extent. For instance, data security and privacy issues with regard to Chinese digital enterprises such as TikTok, Tencent and Alibaba become global focus in the escalating US-China trade war.[19] But for the development of China's data protection law, these foreign forces are not as important as the abovementioned three actors, and their influences can only be effective when those three major actors respond to them.[20]

The above categorization of the major actors can offer an overview of the power dynamics in the development of China's data protection law. But this assessment comes at the cost of a broad brush, at some points lacking detailed discussion of different actors in the same category and the potential conflicts and collaborations between these different actors. For instance, the Chinese state as the major, dominant actor is not entirely a holistic body, but is composed of multi-level entities with different interests and political-legal agendas.[21] Compared with middle and small-sized enterprises , large digital giants have apparently different values and approaches to data privacy protection, and therefore have different power relations with the State. The Chinese central government may also focus on protecting the different values at different times. Such details may not be fully revealed in this Article. However, we believe that the analysis of major actors' power relation and its possible outcomes is a worthy effort for revealing some facts and the underlying rationales in the development of China's data protection law that are missing in the present scholarship.

3. Defining and securing fundamental values

With respect to the development of China's data protection law, the three major actors - the State, digital enterprise and the public, have different, oftentimes conflicting focus in pursuit of the three fundamental values, namely public security, economic growth, and data privacy protection. This section examines these three fundamental values respectively and their complex and multidimensional relationships with the three major actors under the context of China's rapid economic and social progresses.

3.1. *Common consensus: public security as a trump card*

The Chinese state treats public security as an overarching value in IInternet governance.[22] In most cases in China, public security, national security or state security are not clearly distinguished and well defined, but used interchangeably. Preserving public security has been the trump card since the outbreak of the 1989 Tiananmen Square Protests.[23] For the national leadership, upholding the supremacy of public security provides sufficient legitimacy for its governance. To a large extent it also means securing and retaining the present political-legal order, under which the State has tight control of the Chinese society. The current political-legal order has been officially promoted as the precondition of China's social harmony and continuous economic growth, which are supported by the majority of Chinese. Such political ideology is understandable - there is hardly economic growth and prosperity in a state of disorder and chaos.

Thus, over the last three decades, China' public security apparatus has experienced dramatic expansion with regard to bureaucratic rank, institutional capacity and spending.[24] China has undergone a process of widespread "securitization" - virtually every field of public governance has been sucked into the vortex of public security maintenance. Maintaining public security is also one of the two key focuses of Chinese lawmakers (the other focus is fostering market economy). The current development in security maintenance has led the Chinese government to de-emphasize the role of formal law, and to revive pre-1978 court mediation practices. As Carl F. Minzner has warned, such security-oriented develop-

[18] 'Update concerning China's acts, policies and practices related to technology transfer, intellectual property, and innovation', Office of the United States Trade Representative, 2018, pp. 1-8.

[19] One of the major concerns concerning data security issue is the Chinese state's (supposedly) unlimited access to foreign citizen's personal data in case they are transferred back to China or accessible from China, see: Ryan Broderick, 'Forget the trade war, TikTok is China's most important export right now, Buzzfeed News', Buzzfeed News, 2019, < https://www.buzzfeednews.com/article/ryanhatesthis/forget-the-trade-war-tiktok-is-chinas-most-important-export> Accessed 25 July 2020.

[20] For the limited space of this Article and complexity of the issue, this Article will not discuss the foreign influences on the development of China's data protection law, despite the fact that this certainly deserves full academic attention from political-legal aspect.

[21] The lawmaking in post-Mao China is a fragmented, multi-arena process and the political battles over the law drafting usually occur among the Party Centre, the State Council, the National People's Congress and other major actors, see: Murray Scot Tanner, *The politics of lawmaking in post-Mao China: institutions, processes, and democratic prospects* (Clarendon Press, Oxford ,1999), pp. 47-49.

[22] Article 28 of the Chinese constitution states that all behaviors that endanger public order, public security and national security should be punished. For better illustration, we use the term 'public security' in this Article.

[23] For the history of public security/stability preservation in China, see: Chongyi Feng, 'Preserving stability and rights protection: conflicts or coherence? *J Curr Chin Aff* 42 (2013), pp. 22-34.

[24] Yuhua Wang and Carl Minzer, "The rise of the Chinese security state", *China Q* 222 (2015), pp. 339-341.

ments suggest China's turn against the rule of law.[25] Thus the central status of public security is the inborn mega principle in China's cyber law from three major dimensions: cyber security, the Internet's critical role in pursuit of public security, and the populist support for public security. These three major perspectives are discussed below.

First, Chinese lawmakers have recognized that cyber security is an important aspect of public security. The Chinese leadership has oftentimes emphasized the significance of cyber security for Internet development, and has taken various measures to ensure cyber security. In line with the national security policy, China's cyber law has put great emphasis on public security.[26] For instance, the existing criminal justice system moves quickly to adjust to the changes brought up by the expansion of the cyberspace. The Standing Committee of the National People's Congress (NPCSC) amended the Criminal Code four times from 2009 to 2017. The criminal protection against identity thefts now covers both public and private sectors, and the maximum custodial penalty has been upgraded from three years to seven years. According to the Supreme People's Court and the Supreme People's Procuratorate, stealing or other unlawful uses of more than 50 items of sensitive personal data would amount to a criminal offence.[27] While civil and administrative remedies remain underused, the criminal apparatus serves as a relatively effective instrument to fight against data abuse. In 2017, for instance, the number of criminal cases in identity theft reached 4911 (with 15,463 suspects arrested), compared to 1886 cases (with 4261 suspects arrested) in 2016.[28]

For the purpose of improving cyber security, China has enacted a number of administrative laws and regulations to shape Netizens' behaviors. The Chinese government hopes the effective implementation of these laws and regulations could create a more orderly cyberspace and eliminate the threats for public security. Most noticeable laws and regulations are those concerning the comprehensive real-name registration system and the social credit system. These two systems represent Chinese lawmakers' efforts to create a "harmonious society" by limiting cyberspace anonymity and rating the trustworthiness of 1.4 billion Chinese citizens.[29] The by-product of such security-related legislation is diminished individual privacy and freedom of speech against the State. If one views China's cyberspace as the Wild West where the development of Chinese citizens' freedom and liberty are unfettered, he may make a serious mistake. A landmark development for regulating cyber security came in 2016 with the promulgation of the Cybersecurity Law. This Law is characterised by its new data protection requirements that are more comprehensive than those in previous legislation. But the protection in this Law is constructed based on network security and the Chinese government has broad authority to improve the level of security.[30]

Second, the Chinese state has been seeking various technical measures to tackle cyber problems that may threaten public security. A telling example is the suppression of political dissenting opinions against the existing political order. For a long time, China is infamous for strong internet censorship and mass surveillance, including the sophisticated Internet filtering system "Great Firewall" to control online information.[31] By using content-analysis technique and other cutting-edge techniques, Chinese government has created a long blacklist of unwanted keywords, and accordingly blocked a large number of foreign and domestic websites.[32] Since this system is embedded into the Internet architecture, its operation is nearly invisible and less costly compared to physical law enforcement. The successful filtering system in the long run has the cumulative effect of shaping netizens' behaviors and ideology, redirecting many Internet users' interest into online entertainment instead of political information.[33] Another recent example is the wide deployment of facial recognition technologies that allow prediction and real-time reaction to public disorder.[34] While helpful to curb crimes, such wide application of surveillance technologies tends to create a techno-authoritarian state with rising privacy concerns.[35] In the post-digital age, the coming of smart cities and smart

[25] Carl F. Minzner, "China's turn against law", *Am J Comp Law* 59 (2011), pp. 935-936.

[26] See '习近平:没有网络安全就没有国家安全'(Xi Jinping: without cybersecurity there is no national security), 2018, Cyberspace Administration of China, available at <http://www.cac.gov.cn/2018-12/27/c_1123907720.htm> Accessed 25 July 2020.

[27] 《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(the interpretation of the application of law to handle criminal cases regarding the misuse of the personal information of citizens), Supreme People's Court and Supreme People's Procuratorate, 2017.

[28] For the 2016 statistics, see 《公安部召开打击黑客破坏和网络侵犯公民个人信息犯罪专项行动部署会》(The Ministry of Public Security convened a preparation meeting on striking down hacking and offences about personal information), The Ministry of Public Security, 2017, < http://news.sohu.com/20170311/n483000239.shtml> Accessed on 20 July 2020; for the 2017 statistics, see 'Ł'Š2017年公安机关侦破侵犯公民个人信息案件4900余起》(Public security agencies detected more than 4900 criminal cases about misuse of citizen's personal information), Tianjin Cyber-police, 10 January 2018,<https://www.weibo.com/ttarticle/p/show?id=2309404194641007251178> Accessed on 20 July 2020.

[29] See Jyh-An Lee and Ching-Yi Liu, "Real-name registration rules and the fading digital anonymity in China", Wash Int Law J 25(2016), pp. 17-21; Pete Hunt, China's great social credit leap forward, The Diplomat, 2018.

[30] Jyh An Lee, Hacking into China's cybersecurity law, Wake Forest Law Rev 53(2018), pp. 64-67.

[31] Jyh-An Lee and Ching-Yi Liu, Forbidden city enclosed by the great firewall: the law and power of Internet filtering in China, *Minn J Law Sci Technol* 13(2012), pp. 125-129.

[32] ibid., at 131.

[33] James F. Scotton, The impact of new media, in James F. Scotton and William A. Hachten (Eds), *New media for a new China,* (John Wiley & Sons, New York, 2010), p. 32.

[34] Local governments in eastern China like Hangzhou and other cities use facial recognition technologies to monitor Uighers who were treated as an ethnic group with potential threat to public order, See: Paul Mozur, *One month, 500,000 face scans: how China is using a.i. to profile a minority*, the New York Times, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html> Accessed 20 July 2020.

[35] For instance, for quick detection and arrest of criminals in urban areas. See: Tara Francis Chan, *One Chinese city is using facial-recognition that can help police detect and arrest criminals in as little as 2 minutes, Business Insider Nederland, 2018,*

homes in China means that public security forces and law enforcement agencies will rely more on networked, digital means to achieve public security.[36]

Third, Chinese citizens have generally reached a consensus that public security is a fundamental value. Such value is essential for preserving public order and social harmony, serving as the precondition for China's economic success and prosperity.[37] Thus maintaining public security via mass surveillance and other high-tech means is more or less a communal political and legal decision. Chinese government's measures for maintaining public security, especially for tackling terrorist attacks, political and military challenges from "foreign forces" and economic crisis, appear necessary and acceptable.[38] On this matter, backed by the public, the Chinese government has absolute authority in taking public security as the trump card, albeit this could be at the cost of hindering economic growth and infringing upon individual privacy.

3.2. *Growing digital economy and the rise of data power*

The spectacular development of digital economy is one of the most inspiring phenomena in China during the last decade. Such development cannot be achieved without the policy support of the Chinese government and the rise of private digital enterprises who become the principal driving force for ongoing economic development. The favorable policy environment and the rise of digital power jointly pose serious challenges for the development of China's data protection law. This section examines China's development strategies on digital economy followed by an examination of the rise of digital power. Then it concludes that China has been giving strategic priority to economic and technolocial development, with data protetion as a secondary policy goal.

3.2.1. *National development strategies*

Another fundamental value that has long been dictating China's law and policy development since the early 1980s is economic growth.[39] Undeniably, economic growth is a fundamental value in the Chinese society, which just stepped out of poverty recently. The State regards securing stable economic growth as critical to legitimize its ruling. The public generally has substantially benefitted from China's economic growth,[40] thus they are willing to recognize the legitimacy of the present legal order.[41] Though troubled with systematic corruption, social injustice and weak human rights protection, sustainable economic growth provides the necessary material resources for the State to buy off loyalty from supporters, to compensate the weakest, and to maintain political order and public security.

After realizing that the new generation of Information Communication Technology (ICT) has the potential to sustain China's economic growth, the Chinese central government formulated an array of development strategies to provide policy support for ICT development.[42] ICT, which was initially taken as a tool to enhance traditional manufacturing industries, now becomes the hope to transform China into an economic superpower in the near future. Boosting new innovative digital technology has become another concrete goal under the umbrella of economic growth. In the early 1997, the Chinese leadership began to show a welcoming attitude to emerging ICT. In both 2002 and 2003, the National Congress of the Chinese Communist Party (CCP) singled out in two annual reports that "promoting the informatisation of the national economy",[43] and that "industrialization is still a difficult long-term task, and using information technology is an inevitable path to accelerate industrialization and modernization."[44] For implementing these two top Party requirements, the State Council (China's cabinet) issued the "State Informatisation Development Strategy 2006–2020" (2006 Informatisation Strategy).[45] In this Strategy, the State Council highlighted

< https://www.businessinsider.com/china-guiyang-using-facial-recognition-to-arrest-criminals-2018-3> Accessed 20 July 2020.

[36] Ma Alexandra, "China is building a vast civilian surveillance network — here are 10 ways it could be feeding its creepy "social credit system'", Business Insider Nederland, 2018, < https://www.businessinsider.com/how-china-is-watching-its-citizens-in-a-modern-surveillance-state-2018-4> *Accessed 20 July 2020.*

[37] Yang Zhong and Yongguo Chen, Regime Support in Urban China, *Asian Survey*, 53(2) 2013, pp. 369-392.

[38] Bill Birtles, China's security obsession, a point of national pride, ABC News, 2017, < https://www.abc.net.au/news/2017-10-10/chinas-security-obsession-is-now-a-point-of-national-pride/9032518> Accessed 20 July 2020.

[39] The consistent economic reforms after 1978 not only successfully maintained China's rapid economic growth, but also result in a strengthened Party state, see: Mary E. Gallagher, 'Reform and openness": why China's economic reforms have delayed democracy', *World Politics* 54.3 (2002): 338-372.

[40] Xi Jingping Administration has stressed the importance of promoting social justice and equality and boosting social welfare, see: Lam Willy Wo-Lap, *Chinese politics in the era of Xi Jinping: renaissance, reform, or retrogression?* (Routledge, New York, 2015), pp. 185-189.

[41] Rcent research has shown how the elite view of China is distant from the public in diminishing the contribution of economic growth to political legitimacy, see: Ankit Panda, Where does the CCP's legitimacy come from? (Hint: it's not economic performance), the Diplomat, https://thediplomat.com/2015/06/where-does-the-ccps-legitimacy-come-from-hint-its-not-economic-performance/ Accessed 20 July 2020.

[42] One example is the complex industrial guidelines, strategies and subsidies from the Chinese government to boost China's smart, connected car development. See: Bo Zhao, *Connected cars in China: technology, data protection and regulatory responses, in* Grundrechisschutz im smart car: kommunikation, sicherheit und datenschutz Im vernetzten fahrzeug, Alexander ROßNagel and Gerrit Hornung (Eds.), (Springer, New York, 2019), pp. 417-438.

[43] 《高举邓小平理论伟大旗帜, 把建设有中国特色社会主义事业全面推向二十一世纪, 在中国共产党第十五次全国代表大会上的报告》(Upholding the great banner of Deng Xiaoping theory and advancing the cause of building socialism with Chinese characteristics into the 21st century– report on the 15th National Congress of the CCP), the 15th central committee of the Chinese Communist Party, 1997.

[44] 《全面建设小康社会, 开创中国特色社会主义事业新局面》(Building a well-off society in an all-round way and create a new situation in building socialism with Chinese characteristics -report on the 16th National Congress of the CCP), the 16th Central Committee of the Chinese Communist Party (CCP), 2002.

[45] 'Ł'Š2006-2020年国家信息化发展战略》(State informatisation development strategy 2006-2020), General Office of the CCP Central Committee and General Office of the State Council, 2006.

the importance of data, defining it as "an important production factor, virtual asset and wealth of society".[46]

In 2015, the Xi Jinping administration started to improve the policy support for informatisation and issued a number of key development strategies. Among these strategies, the most well-known one is the 'Made in China 2025'. Corresponding to Germany's Industry 4.0, 'Made in China 2025' is intended to transform China from a large manufacturer (in terms of quantity) into a strong manufacturer (in terms of quality) by 2025.[47] The deadline of 'Made in China 2025' is only intermediate, with an ultimate goal of transferring China into one of the most advanced and competitive manufacturers in the world by 2049.[48] This strategic Plan targets a wide range of key areas: next-generation information technology, including 5 G networks and cybersecurity; high-end numerical control tools and robotics; aerospace; ocean engineering; advanced railway equipment; energy-saving and new-energy vehicles; power equipment; agricultural machinery; new materials; biomedicine and high-performance medical devices.[49]

Usually such industrial strategic plans come with specific implementation measures for full implementation, which is well rooted in China's long tradition of planned economy. For instance, China's 13th Five-Year Plan for Economic and Social Development (drafted in 2016) listed ICT as the highest priority sector for future development. Section Six is entitled: "expanding cyber economic space" with the first task of "building ubiquitous and efficient information networks". This targets three main areas: new generation high-speed fiber-optic networks, advanced and ubiquitous wireless broadband networks, and new information network technology focusing on cloud computing and high-end industrial software.[50] Shortly after, the State Council issued an informatisation-specific Five-Year Plan that outlined the key development areas and specifying 12 accompanying priority tasks, designated 74 specific projects, and designated the ministries and committees responsible for the implementation of these projects.[51] Such national level strategies can be executed with specific sectoral plans by different supervisory and governing bodies.

Further, specific strategies have been made to facilitate technology development in relevant areas, such as big data and data analytics. Two noticeable strategies on big data are "the Outline of Action Plan for Promoting Big Data Development" issued by the State Council (August 2015),[52] and "Plan for Big Data Development" issued by the Ministry of Information and Industry Technology (MIIT, 2016).[53] Both of these two strategies recognize big data as "an important and fundamental strategic state resource", is "a new engine that will accelerate economic transformation and reshape the State's competitiveness", and is "a new path for enhancing the government's governance capacity".[54] With respect to Artificial Intelligence (Al), the State Council has issued the Artificial Intelligence Development Guide. This Guide defines Al as a driving force for China's industrial transformation and a new engine for China's economic growth, with the ultimate goal to make China a world center for Al research and development by 2030.[55]

In reality, the above strong ICT development strategies have profound impacts virtually on every aspect of social and economic life in China.[56] They tend to create strong momentum to achieve the designated middle-term goals of comprehensive technological upgrading in targeted sectors. Venture capitals and other non-governmental investments flow into the policy-favored sectors for profits, taking advantages of national policy. Local governments also tend to quickly jump on board to exploit policy bonus such as central government's subsidies. Private entrepreneurs respond swiftly to gain governmental subsidies and supportive loans. How significant these industrial strategies and planning schemes may indeed stimulate data-driven economy development is debatable among scholars and politicians. However, even cautious foreign observers admit that China is likely to succeed in elevating certain key manufacturers to the positions of fierce competitors at the global market.[57] Another important aspect worth mentioning is the contribution and commitment of Chinese local governments in attracting investment and digital enterprises to stimulate local economy and employment. With greater discretion designated by the central government, these local governments grant investors rather lax, favorable local policies and regulations, often with large tax cut (or zero tax) and even free land use.

3.2.2. *The rise of digital power*

UndUnder Under the very favorable policy environment, Chinese private technology companies have grown into global leading players mainly due to their fast expansion in China's domestic market (and thus with surplus capital to invest else-

[46] ibid.

[47] Jost Wubbeke, Mirjam Meissner, Max J. Zenglein, Jaqueline and Bjorn Conrad, "Made in China 2025, the making of a high-tech superpower and consequences for industrial countries", Mercator Institute for China Studies, 2016, <http://www.documentcloud.org/documents/3864881-Made-in-China-Paper.html> Accessed 20 July 2020.

[48] ibid., at p17.

[49] David Dodwell, 'The real target of Trump's trade war is 'made in China 2025', South China Morning Post, 2018, <https://www.scmp.com/business/global-economy/article/2151177/real-target-trumps-trade-war-made-china-2025> Accessed 20 July 2020.

[50] 'Ł'Š'¸'-Ž'^'º'º'"'…'±''Œ','½','½'°"'»'–'µ'^''Œ'¤'¾'¼'š'–"'±'•'¬'¬'Ž''¸'‰Meissner§Max J. Zenglein, Jaqueline and Bjorn Conrad, "Made in China 2025, the making of a high-tech superpower and consequences for industrial countries", Mercator Institute for China Studies, 2016, <http://www.documentcloud.org/documents/3864881-Made-in-China-Paper.html> Accessed 20 July 2020.

[51] 《十三五国家信息化规划》[(the 13th five-year informatization plan) State Council, 2016.

[52] 'Ł'Š'¿'ƒ'¿','¤'§'•'°'Ž'®'–"'±'•'¡'Œ'Š'"'º'²'¦''Ł'‹(Outline of action plan for promoting big data development)] State Council, 2015.

[53] 'Ł'Š'¤'§'•'°'Ž'®'º'§'¸'š'–"'±'•'§','„'^''Ł'‹(Plan for the big data industry) Ministry of Industry and Information Technology, 2017.

[54] ibid.

[55] 《新一代人工智能发展规划》[(The development plan of the new generation artificial intelligence) State Council, 2017.

[56] Omer Tene and Jules Polonetsky, Big Data for all: privacy and user control in the age of analytics, *Northwest J Technol Intell Property 11(2013), pp. 243-251.*

[57] For the prospects of these strategies, see Jost Wubbeke, Mirjam Meissner§Max J. Zenglein, Jaqueline and Bjorn Conrad, "Made in China 2025, the making of a high-tech superpower and consequences for industrial countries", Mercator Institute for China Studies, 2016, <http://www.documentcloud.org/documents/3864881-Made-in-China-Paper.html> Accessed 20 July 2020.

where). Alibaba Group Holding and Tencent Holding are on the list of the ten most valuable technology companies in the world.[58] By far, China is one of the two countries where unicorn start-up companies are most concentrated (with 98 in total).[59] The only qualified competitor is the United States with 166 unicorn start-up companies.[60] Apparently, a number of technology enterprises (such as Huawei and Xiaomi) have been selling their products and services in both developed and developing countries, ranging from India, Southeast Asia, and most African countries.

The rise of private digital companies has made tremendous changes to the Chinese society. The new digital technologies have overhauled a number of traditional industries. Nowadays in China, virtually all of the key traditional industries have been upgrading with the help of information networks and data analysis. These companies have brought the majority of Chinese people, including those in rural areas, into the online world, engaging with social networking activities and e-commerce on daily basis.[61]Perhaps more important is that these private digital companies have fundamentally transformed China's pubic governance and state-society relationship. Such transformation is observable in two aspects.

First, the Chinese state can directly engage, respond to and interact with the public through various online platforms. E-mail, Microblog, Wechat and other online channels enable the State to solicit public opinions on law/policy making in an unprecedented manner. More importantly, the State seeks wide-ranging and multi-level cooperation with digital companies for realizing different regulatory goals. The main purpose of that cooperation is to use digital enterprises' technological tools and data power. A new legislative trend for such cooperation is the increasing government power to access data that held by digital enterprises. The 2019 E-commerce Law requires platform operators to hand over their business tenants' identity data to the market regulatory authority and taxation data to the taxation authority(Article 28). The 2018 'management measures on the supervision platform for online taxi booking business' adopted by the Transport Ministry requires online taxi-booking business operators to comply with the following obligations: update its static information to the supervision platform within 24 h, upload operating data concerning order, vehicle, driver, passenger, service quality, and customer evaluation within 300 s, and upload passengers' whereabouts data within 60 s.[62] The Chinese government needs more support and cooperation from these digital enterprises to achieve its governance goals. Such needs allow the digital companies to gain more bargaining power in shaping the state-enterprise power relations. The independence of the digital companies has further helped them to establish various communicating channels with Chinese governments at both the central level and local levels to protect corporate interests in informal ways.

Second, the founders of these technology companies are active in participating China's political life, at both the local and central levels, with rather obvious influences.[63] For instance, leaders of China's top digital giants such as Jack Ma (Alibaba), Pony Ma (Tencent) and Robin Li (Baidu) often accompany President Xi Jinping to visit the EU and the US. In recent years, they also tend to more proactively participate in China's law-making process via the channel of "two session" (namely the NPC and the Chinese People's Political Consultative Conference). On behalf of technology companies, deputies in these two sessions have proposed multiple policy motions, aiming to influence the policy/law-making on the digital economy.[64] Digital giants such as Tencent and Alibaba have established their own think tanks and research institutes, to publicize and promote certain economic theories or perspectives to influence the public and policy makers.[65] These enterprises are also very active in participating State-led or State-coordinated research projects, focusing on certain technological developments including.[66] Another important issue is the emergence of various industrial associations at both national and local levels, which serve for multiple purposes such as promoting sectoral interests, establishing quasi-official communication channels with the government, and

[58] See: 'These are the most valuable tech companies of 2019', GQ Staff, 17 December 2019, < https://www.gq.com.au/success/career/these-are-the-most-valuable-tech-companies-of-2019/image-gallery/cb12dd280d9792727c75d9dbc769e4fb?pos=2> accessed 20 July 2020.

[59] A unicorn startup or unicorn company is a private technology company with a valuation over $1 billion. For the detail information about the unicorn in the world, see the Global Unicorn Club, 2019, <https://www.cbinsights.com/research-unicorn-companies> Accessed 20 July 2020.

[60] For the list of the unicorn startup companies in the world, see websites of Cbinsights, <https://www.cbinsights.com/research-unicorn-companies> Accessed 20 July 2020.

[61] by the end of 2018According, China's Netizen population has reached 829 million. 817 million of them is able to access the Internet by smart phone, see '第43次中国互联网络发展报告' (the 43rd China Statistical Report on Internet Development) China Internet Networks Information Center <http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/> Accessed 20 July 2020.

[62] 《网络预约出租汽车监管信息交互平台运行管理办法》 (Management measures on the information exchange platform for online taxi hailing services), Transportation Ministry, 2018.

[63] Many Chinese digital giants such as Huawei and Alibaba are private enterprises, which is contrast to the allegation of many western Media, even though their owners may have close ties with the Chinese government.

[64] According to Deng and Kennedy, since 2010 there is a growing recognition that business lobbying is an integral part of the country's policy process at both the local and national levels, mostly under the umbrella concept of "interest groups", see Guosheng Deng and Scott Kennedy, Big business and industry association lobbying in China: the paradox of contrasting styles, *China J* 63(2010), pp. 101-125.

[65] Among these institutes, most noticeable is the Tencent Internet Research Institute, which publish research articles and reports on data economy and data protection law reviews. See: its website <https://www.tisi.org/> Accessed 20 July 2020. Also Alibaba has set up an advanced research school called DAMO Academy in 2017 to "dedicated to exploring the unknown through scientific and technological research and innovation", see its website <https://damo.alibaba.com/about/> Accessed 20 July 2020.

[66] For instance, Robin Li, the founder and CEO of Baidu, called for the State to endorse the cooperation among leading Chinese companies and to have "national team" to undertake the development of new open innovation platforms in AI, which was followed in state industrial strategy later. See: Elsa Kania, 'China's AI agenda advances', The Diplomat, 2018, <https://thediplomat.com/2018/02/chinas-ai-agenda-advances/> Accessed 20 July 2020.

shaping policy-law making via legislative procedure.[67] Their formal political participation, along with the informal ways mentioned above, is driven by the pursuit of their own corporate interests, or sometimes of public interests in general when the two interests overlap.

In sum, with China's digital economy becoming the dominating model of China's future economic development, the State has to treat the rising digital power (and the big capital flows behind) with increasingincrea respect. The rising digital enterprises has gradually gained the capacity to influence China's policy making agenda, and to construct certain economic and cultural environment in favor of industrial interests.[68]

3.2.3. *Economic and technological development first, data protection second*

However, strong national policy initiatives and support for digital economy may pose serious challenges for developing a better data protection law in China. Two main challenges are most noticeable. First, most industrial development strategies and polices pay insufficient attention to data protection. With rather light touching, the requirements on data security are generally short and ambiguous with no specific objectives and completion dates. Two examples are provided below. The first example is the 2006 State Council's Informatisation Strategy. Although this Strategy spells out the requirement of 'accelerating the legislation on informatisation', this general requirement is listed under the "safeguard measures" section, rather than the "strategic objective" or "key task" sections, suggesting that data security is a secondary value in the Strategy.[69] The second example is the 2015 State Council's Outline of Action Plan for Promoting Big Data Development. Although this Outline urges to accelerate the making of laws and regulations on big data, it lays out rather general legislative plans, and fails to formulate specific objectives and tasks as it did to the planning of data industrial development.[70]

Second, the ambitious short-term goals coupled with relatively limited time for execution, tends to further hinder tipping for good balance between industrial development and data protection. For example, only five years remain to achieve the comprehensive development objectives set by the 'Made in China 2025'.[71] Another example is the 2016 Plan for the Development of Big Data, which requires that seamless data flow between various governmental agencies should be achieved by the end of 2017, and that a "unified open platform for nationwide government data" be in place by the end of 2018.[72] Such limited time for achieving these aims is likely ends up with hasty implementation, creating high pressure for Chinese lawmakers who may not have enough time to respond to new privacy and data protection challenges arising from the accelerated development of new digital technologies. Thus, hasty implementation can be helpful for boosting industrial developments, but at the expense of data privacy.

Third, the large digital enterprises are not in favor of a strong data protection regime that would somehow constrains their business development. Under the favorable policy environment, digital enterprises do not have no strong motive to upgrade their level of data protection. On the contrary, they tend to avoid fulfilling data protection duties as much as possible. On this point, the drafting of China's E-Commerce Law serves as a salient example. The first draft, which incorporated extensive data protection duties for E-commerce operators, had sparked heated controversial debate.[73] During the subsequent drafting and deliberation session at the NPCSC, some deputies recalled that the voice in favor of digital enterprises are the loudest.[74] Despite some deputies called out: "do not damage customers' rights and interests for supporting the development of E-commerce operators", the voices for supporting E-commerce operators finally prevailed at the later stage of the drafting process.[75] The final version, which was promulgated by the NPCSC in August 2018, removes all the data protection requirements for E-commerce operators.

Last, the fast technological advance in China, resulting from the strong ICT development strategies and enterprises' pursuit of best profits, has adversary effects on the development of data protection law. Previous study warns that the current advances in ICT technology tends to offer the government and high tech companies unprecedented powers to profile ordinary individuals on a large scale.[76] For example, the development of re-identification technologies tends to disrupt traditional privacy rules, which are based on the assumption that data privacy can be effectively protected by anonymiza-

[67] Compared to the past, such industrial associations have become more independent and self-regulatory, See: Jianxing Yu, Jun Zhou and Hua Jiang, *A path for Chinese civil society: a case study on industrial association in Wenzhou, China* (Lexington Books, Lanham, 2012), pp. 25-26;The reform has been further continued even till recent years with difficulty but obviously turn to be successful with firm determination of the central government to cut off personnel and financial connections between government and trade associations. See: Nectar Gan, Beijing to cut its ties to trade associations, South China Morning Post, 2015, < https://www.scmp.com/news/china/article/1835512/beijing-cut-its-ties-trade-associations>, Accessed 20 July 2020.

[68] Digital companies, for example, attempt to promote the "996" working culture. "996" refers to 12 hours' working time a day (starts at 9 am and ends at 9 pm) with six days a week, see: Denise Hruby, Young Chinese are sick of working long hours, BBC Worklife, 2018, < https://www.bbc.com/worklife/article/20180508-young-chinese-are-sick-of-working-overtime> Accessed 20 July 2020.

[69] See'Ł'Š2006-2020年国家信息化发展战略》 (State informatization development strategy 2006-2020)]General Office of the CCP Central Committee and General Office of the State Council, 2006.

[70] ibid.

[71] 《中国制造2025》 (Made in China 2025) State Council, 2015.

[72] 《促进大数据发展行动纲要》 (Outline of action plan for promoting big data development) State Council, 2015.

[73] The data protection duties are incorporated in Articles 45 to 52 of the draft E-commerce Law. Article 45 of this draft law states: "a user of E-commerce enjoys the right to self-determination of her/his personal data".

[74] Cong Zhang,《各方权益保护需要平衡》 (Different Interests need to be balanced), 人民日报(People's Daily), 2016.

[75] Xiaolei Pu, 《不能因过度保护电商而损害消费者权益》 (The Law should not excessively protect E-commerce operator at the expense of the interest of customers) 法制日报(Legal daily), 2016.

[76] Paul Ohm, Broken promises of privacy: responding to the surprising failure of anonymization, UCLA Law Review 57 (2010), pp. 1703-1706.

tion technologies.[77] In China, cross-platform data sharing and processing are very popular.[78] The government is also infamous for increasing its access to privately-held data via legislative measures.[79] The development of privacy-intrusive technologies combined with the expansion of big databases would largely enhance government's surveillance power at the expense of individual privacy, posing serious challenges to China's legislative move on data protection.[80]

3.3. *Deepening digitalization, escalating privacy concern*

With the deepening digitization and connectedness of the Chinese society, ordinary Chinese citizens have suffered from data abuse/misuse and privacy breaches. The widespread cybercrimes are attributed to a number of factors, including fast intrusive technology developments, privacy-unfriendly corporate culture, poor law-policy protection, and a weak privacy culture in Chinese society.[81] Abuse and misuse of personal data is rampant across the country, which occurs in corporate practices, and massive public surveillance. Data breaches have led to suicide, reputation bankruptcy, and various internet related criminal activities. In addition to large-scale data leak incidents from digital enterprises, the data abuse and misuse by government officials are never rare in China.[82] Personal data are deemed as assets for various purposes, including targeted advertisements (such as finance and real estate marketing), private debtor collection, and private detection. More recently, with the promotion of smart cities and Internet of things in China, social members have no choice but to be connected to the Internet and thus data privacy has become a big concern even among ordinary Chinese.[83]

It is true that the modern concept of privacy is alien to traditional Chinese culture, which is largely of a collective nature even until the recent time. However, with Chinese people's life largely moved into cyberspace, data privacy has become a growing concern for ordinary Chinese citizens after experiencing and witnessing privacy harms.[84] The most noticeable changing point that has awakened ordinary Chinese of their losing control of life, perhaps comes from the outbreak of an array of recent tragedies and scandals that were all triggered by data abuse. In this context, the escalating need for better privacy and data protection from consumers and crime victims cannot be overlooked by the State and corporate force. A landmark case is the death of Yuyu Xu in 2016. This eighteen-year-old high school graduate in Shandong province died as a victim of a wire fraud of about 9000 Yuan (1250 euro). Xu's death sparked nationwide outcry and led to quick detection and prosecution of the suspects.[85] Xu's case and other similar ones lead to public outcry for better data security and data privacy, especially among young internet users. Those who were born after middle 90′s, are rather liberal and born digital, growing up with the Internet in China. Empirical research shows that the young generation of Chinese, especially university students, have ascending privacy concerns, when they use social networking services such as Wechat, worrying most about financial data leak, privacy breach, and personal data leak.[86]

Similar to Western societies, the growing concerns and need for more privacy protection in China are often compromised by the desire for convenience and economic benefits. The privacy-for-data tradeoff happens often in Chinese society given that Chinese internet users has less privacy concerns.[87] But eventually they have to pay back in one way or another. The common consequences of data leak include psychological distress, physical damage, and financial loss. Borrowing Alan Westin's words, the majority of Chinese belong to the group characterized as either privacy pragmatists or privacy unconcerned.[88] Unlike Western consumers, Chinese

[77] Ibid, at 1716-1717.

[78] Xiang Yang, Li Wang, Jianwei Qian and Xiaoyang, 'Can China lead the development of data trading and sharing market?', *Commun ACM*, 61 (2018), pp. 50-51.

[79] For instance, the implementation of new social credit system would result in the collection of huge amount of data by the government, see: Yongxi Chen and Anne S. Y. Cheung, The transparent self under big data profiling: privacy and Chinese legislation on the social credit system, *J Comp Law* 12 (2017), pp. 356-378.

[80] Amir Gandomi and Murtaza Haider, Beyond the hype: big data concepts, methods, and analytics, *Int J Inf Manag* 35 (2015), pp. 137-144.

[81] See: Luisa Tam, 'Why privacy is an alien concept in Chinese culture', South China Morning Post, 2018, < https://www.scmp.com/news/hong-kong/article/2139946/why-privacy-alien-concept-chinese-culture>, Accessed 20 July 2020.

[82] Starting in 2017, Government agencies have recently become a target of criticism by social media for failing to provide adequate protection for personal information collected, see Wan Jing, " ⟨11:cjk ⟩'š'–'µ'£'-'‰'ƒ'"'^'†'"'¿'º'œ'½''«'™'³'„'œ'² '…'¬'º''š'†'§''¿'¡''˜⟨/11:cjk⟩ (The websites of some local governments in Anhui and Jiangxi provinces divulge citizen's private information) 法制日报 (Legal Daily), 2017; Zhang Guifeng, "政府网站更应做好个人信息保护 (Government website should be a model for personal information protection) 湖北日报 (Hubei Daily), 2017; Yang Qiang, "政府网站泄露个人信息事件追踪 (Report on the events of divulging personal information by government website) 重庆日报 (Chongqing Morning Daily), 2017.

[83] Fan Yang and Jian Xu, Privacy concerns in china's smart city campaign: the deficit of China's cybersecurity law, *Asia Pac Policy Stud* 5 (2018), pp. 533-543.

[84] The Internet has created a common living space for human communities, and information privacy is more and more a global, internationalized phenomenon regardless of cultural and ethnical backgrounds. See: Bo Zhao, The internationalization of information privacy: towards a common protection, *Gron J Int Law* 2 (2014), pp. 1-3.

[85] Fraud case of Zheng Wenqiang and Chen Fang (《郑文强,陈访诈骗案》) (2017) (鲁1311刑初333号).

[86] Qi Shen, 《风险与成本的权衡:社交网络中的"隐私悖论" ——以上海市大学生的微信移动社交应用 (APP) 为例》 (Balancing risk and cost: the privacy paradox in the social network, the case of WeChat application in Shanghai undergraduates) ,《新闻与传播研究》 (News and Communication Research) 8 (2017), p. 61.

[87] Wang Yang, Huichuan Xia, and Yun Huang, 'Examining American and Chinese Internet Users' Contextual Privacy Preferences of Behavioral Advertising', *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, ACM, 2016, pp. 539-542.

[88] Alan Western, Opinion surveys: what consumers have to say about information privacy, 2001, hearing before the subcommittee on commerce, trade and consumer protection of the committee on energy and commerce house of representatives, 2001, < https://www.govinfo.gov/content/pkg/CHRG-107hhrg72825/html/CHRG-107hhrg72825.htm>, Accessed 20 July 2020.

consumers are in a comparatively weaker position (as a legal and economic group), mainly because of discounted human right protection and a unworkable democratic system.

The Chinese state's current response to the escalating public demand for better data privacy protection is not motivated by protecting privacy as a fundamental right, but more for stability and economic reasons. Both the State and digital enterprises have well realized that gaining more public trust and credibility on data privacy protection is essential for the growth of China's digital economy. Accordingly, the need for data protection partially overlaps with the economic interests of the State and digital giants. Thus in this context, data privacy protection recently becomes important in China's legislation and law enforcement. Since 2009, Despite receiving slow and limited responses, the NPCSC deputies have continuously sent law-making motions to the Chinese People's Political Consultative Conference and the NPC.[89] Scholarly discussion over China's future data protection development has been on the rise.[90] Large digital enterprises have openly promoted the importance of data protection, and the State has also frequently conducted nationwide propagandas and educational works on network security via various distributing platforms and channels, including traditional newspapers, official websites, microblogs, radio and TV.[91]

The Chinese government also started to enhance data protection in 2012 with the adoption of an array of statutes and regulations. The major statutes include the 2012 Decisions on Strengthening Information Protection on Networks, the 2015 Ninth Amendments of the Criminal Code, the 2017 Cybersecurity Law, and the 2020 Civil Code. It is noticeable that the Civil Code recognizes the right to data protection as a separate civil right. For implementing the punitive rules of the Criminal Code, the Supreme People's Court and the Supreme People's Procuratorate jointly issued the 'Interpretation on the Application of Laws regarding Criminal Cases violating Citizens' Right to Personal Information' in 2017. This interpretation lays out detailed rules for determining what kinds of data theft is criminally punishable. The legislative efforts to improve data protection was reinforced in September 2018 when the NPC updated its five-year legislative plan. This new plan, for the first time, put the Data Security Law and Personal Information Protection Law onto the first of its three lists that await drafting and deliberation. According to the five year legislative plan, these two laws 'should be submitted to the NPCSC for deliberation by March 2022'.[92]. Drafting these two comprehensive laws suggests that China's legislative development on data protection has entered into a new stage although whether these proposed laws can be promulgated on time remain uncertain.[93]

To further enhance China's data-driven governance and economy, the Chinese government has also launched socio-legal campaigns, trying to improve privacy awareness among ordinary Chinese time and again. As many scholars observed, ordinary Chinese citizens have been given more data protection against excessive data use by the government and digital enterprises.[94] Though applausive, the continuous commitment to improving data privacy protection in China cannot be attributed to fulfilling the legal requirement on rights protection given that data privacy is not a fundamental right.[95] The right protection improvement only happens in areas where the State, digital enterprises and the public have coincidently reached a consensus.[96]

Confronting the social and political pressure from both the Chinese society and government, the private sector's commitment to privacy and data protection has been half-hearted. Such commitment is easily interrupted by digital enterprises' desire for higher profits and by the market competition, which is featured by the popular practice of "racing to the bottom" (usually lowering price). More or less, data privacy protection is merely window dressing, as demonstrated in the "shameless" statement made by Robin Li as mentioned earlier.[97] Li's statement shows a top entrepreneur's perception on the Chinese public's privacy psychology in a much candid manner, although politically incorrect. The popular vehement critique against Li denotes the public's lack of trust in the private sector.

On the whole, the State and digital enterprises have common interest in improving data privacy protection only when it can bring political and economic benefits. In this context, the State and digital enterprises stand on the same side with

[89] Xianzhong Sun, '关于尽快制定我国个人信息保护法的建议'(Suggestion concerning enacting the personal information protection law) Chinese Law Forum, 2017, <http://www.iolaw.org.cn/showNews.aspx?id=60931> Accessed 20 July 2020.

[90] Some recent discussions include Zhang Xinbao, 《从隐私到个人信息:利益再衡量的理论与制度安排》 [From privacy to personal information, the theory of interest re-balance and regulatory framework] 中国法学 [China Legal Science] 3 (2015), pp. 38-59; Gao Fuping, 个人信息保护:从个人控制到社会控制 [Personal information protection: from individual control to social control] 法学研究 (Chin J Law) 3(2018), pp. 84-101; Zhou Hanhua, 《探索激励相容的个人数据治理之道》 (Exploring the personal data governance that achieve incentive compatibility) , '³'•'-'¦' '"©'¶(Chin J Law) 2(2018), pp. 3-23.

[91] 《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>实施情况的汇报》(Report on investigating the enforcement of the cybersecurity law of the People's Republic of China and the decision on strengthening information protection on networks) NPCSC Investigation Team, 2017.

[92] '十三届全国人大常委会立法规划'(The legislative plan of the 13th NPCSC, Xinhua News, 2018, Available at <http://www.gov.cn/xinwen/2018-09/08/content_5320252.htm> Accessed 20 July 2020.

[93] Yang Feng, The future of China's personal data protection law: challenges and prospects, *Asia Pac Law Rev* 2 (2019), pp. 18-20.

[94] Samm Sacks and Lorand Laskai, 'China's privacy conundrum', Slate Magazine, 2019 <https://www.pogowasright.org/chinas-privacy-conundrum/> Accessed 20 July 2020.

[95] Although considerable progress has been made consistent with China's economic developments and opening to the outside world, the human rights protection is problematic in the context of the Party State. See: *Ann Kent, China, the United States, and human rights: the limits of compliance* (University of Pennsylvania Press, Philadelphia, 1999), pp. 194-198.

[96] For a discussion of performance legitimacy see: Hongxing Yang and Dingxin Zhao, State autonomy and China's economic miracle, J Contemp China 24 (2015), pp. 64-82.

[97] Xinmei Shen, Chinese internet users criticize Baidu CEO for saying people in China are willing to give up data privacy for convenience, Netizens Call Robin Li's Comment 'shameless', Abacus, 2018, < https://www.scmp.com/abacus/tech/article/3028402/chinese-internet-users-criticize-baidu-ceo-saying-people-china-are>, Accessed 20 July 2020.

respect to the instrumental value of data privacy protection. The main difference between these two actors is that the State might choose to genuinely protect individual data privacy for fearing that the weak data protection might cripple China's data economy. But the private digital enterprises have no incentive to safeguard the overall data economy and their support for better data protection might be merely lip service in practice. On the corporate side, Huawei, Tencent, Alibaba and other Chinese digital giants eagerly seek to expand overseas, especially in the US and EU markets. They confront constant data protection and national security challenges when foreign user's data can be transferred to China or/and accessible from China. For many in the west countries, such transform of personal information will lead to state surveillance and the infringement of fundamental rights, or even further, aggregating to a big threat to global democracy.[98] The frustration and potential economic loss may motivate these Chinese digital corporations to push for better data protection legislation and practices in China, in particular procedural constrains on state's access to personal data. While encountering reputational crisis because of low level of data protection, China's economic loss would continue to grow. Therefore, the Chinese state must respond to those digital giants' complaints. These digital giants are not only deeply engaged in China's politics but also generate considerable revenues and job opportunities. However, again, how far this enterprise-driven development on data protection may go and in which directions are all to be decided by the Chinese state after balancing many important political, diplomatic and national interests. Certainly, the growing popular demand from all sides for better protection of personal data might serve as an important, long-term driving force for creating a workable data protection regime that could provide meaningful protection. However, to what extent this bottom-up approach can shape China's lawmaking process is unknown under the present political-legal framework. This bottom-up approach has three main limitations.

First, the grass-root voice is difficult to influence China's lawmaking process. China lacks a genuine electoral democracy, and the connection between NPC deputies and their constituents are very weak. The appointment of the key positions at the NPC and NPCSC is still made in accordance with the nomenklatura system and controlled by the Chinese Communist Party's Central Committee.[99] Moreover, because of their large size, short meeting duration and perfunctory legislative procedures, it is difficult for the NPC and NPCSC to conduct meaningful deliberation work.[100] Therefore, the lawmaking process has been largely dominated by party-controlled players mainly from Central Communist Party organs, key NPC officials, NPC's sub-committees and State Council ministries. The ordinary Chinese citizens and even these ordinary NPC deputies seem to be "the silent majority" with little influence in the drafting process.

Second, only in some radical occasions, the public demand can be transformed into a decisive force in the legislative processes, and such transformation is not a normal measure. As evidential in the Sun Zhigang case, the outbreak of significant social incidents and the strong advocacy of enlightened citizens may influence the policy/law development in some occasions.[101] The costs of this kind of populist legislative development, however, have been considerably high, usually involving the loss of human lives to spark nationwide rage, creating huge political-societal pressure for the State to take legislative actions. Many other incidents, which are less radical but happen more frequently, usually do not aggregate such political pressure strong enough for direct political or legal response from the central government. Moreover, the outbreak of such incidents and their social impacts are highly unpredictable. No one knows when such incident will happen and what results they may lead to. Given that most social media in China are controlled by the State, the incurred political pressure could be easily silenced if the State wants to.

Third, it is unlikely to create constitutional protection for data privacy protection by court's interpretation. The current Chinese constitution does not explicitly recognize the right to privacy. The constitutional protection of privacy in the United States was developed through case law during the 20th century.[102] Could China, like the United States, take the case law approach to create a constitutionally protected right to privacy? The answer would have to be no – it is currently not possible to develop a constitutional right to privacy through case law in China. It is well known that the Qi Yuling case is the landmark case in China's constitutional law development. The judge directly referred to the constitutional provisions concerning the right to education as the basis of judicial adjudication. Unfortunately, the Qi Yuling case has no follower.[103] The hope for the judicialization of the China's Constitution finally dies out in 2016, when the Supreme Peo-

[98] In the US, legislators want to further ban "other" Chinese companies besides these famous digital giants. See: Frank Konkel, Report warns of tech threats from 'other' Chinese companies, Nextgov.com, 2020, < https://www.nextgov.com/cybersecurity/2020/02/report-warns-tech-threats-other-chinese-companies/163299/>, Accessed 20 July 2020.

[99] John P. Burns, 'The Chinese Communist Party's Nomenklatura system as a leadership selection mechanism: An evaluation, in Kjeld Erik Brodsgaard (Eds), *Critical readings on the Chinese Communist Party* (Brill, Leiden, 2016), pp. 481-488.

[100] Tony Saich, Governance and politics of china (Palgrave Macmillan, New York, 2011), p. 125.

[101] The miserable death of Sun Zhigang, a 27-year-old college graduate, in the Guangzhou Custody and Repatriation Center in March 2003, directed a nationwide outcry to the age-old system of Custody and Repatriation for Vagrants and Beggars (CRVB) (收容遣送). Following the nationwide outcry and the submission of a suggestion letter for abolishing the CRVB by three legal scholars, the State Council finally abolished the CRVB system. The Sun Zhigang case represent the possibility of the enlightened citizens to successfully accelerate legal reform. But the Sun Zhigang model is not common for China's law development. See: Zhang Qianfan, 'A constitution without constitutionalism? The paths of constitutional development in China', 8 (2010) *Int J Const Law*, pp. 968-971.

[102] For a summary on the early development of the constitutional right to privacy in the United States, see: Jed Rubenfeld, The right of privacy, *Harvard Law Rev* 102 (1989), pp. 744-750.

[103] For the limited development of China's judicial review, see Keith Hand, Resolving Constitutional Disputes in Contemporary China, University of Pennsylvania East Asia law Review 7(2012), pp. 83-85.; Guobin Zhu, Constitutional review in China: an unaccomplished project or a mirage? *Suffolk Univ Law Rev* 43 (2010), pp. 625-626.

ple's Court issued a regulatory document, formally forbidding direct citation of constitutional provisions by courts.[104]

4. Shifting power dynamics and future paths

Possessing different, sometimes conflicting core values, the three major actors has formed complex power relations. The changing power relation would directly influence the development of China's data protection law. After analyzing their dynamic power relations, this section outlines three possible paths of the development of China's data protection law and discusses each path's possible implications for the protection of individual's data privacy.

4.1. *Shifting power relations*

Taking the above full landscape into account, the power relation in the development of China's data protection law has been under constant change. At some times, the interests of the three major actors might overlap with each other. But at other times, conflicts arise between these three actors. The details of their sophisticated relation are reflected in the following aspects.

The State has grown stronger than ever before, possessing increasing technological power and financial resources to achieve its political and economic goals. With high economic growth for decades, the State has gained wide public support, especially when previous widespread corruption has been curbed largely under Xi's ruling.[105] For the time being, the State is still the leading power in regulating data protection. It will continue to treat public security (including Cybersecurity) and economic growth (now the data-driven economy) as the paramount priorities, which are crucial for its political survival and economic success. In the eyes of the State, the order of importance among these three values would undoubtedly be data security, economic growth, and data privacy protection. In case of conflicts, the State would undoubtedly opt for the security even at the expense of data security and privacy protection.

The State tends to deem data protection legislation more as an instrument for upholding public security and facilitating economic growth, than for protecting individual data privacy. On the one hand, the State will act to curb aggressive corporate data-processing practice for preserving public security and retaining the public trust in the data driven economy. On the other hand, it may also need to side with, and even depends technically on large digital enterprises to implement public security policies. Therefore a more lenient data protection strategy is desirable by both the State and the digital enterprises. Such strategy should not obstruct their economic interests and technology developments, especially those based on data processing such as big data and data analytics, AI, facial recognition technology, etc.

The recent acceleration of data protection legislation should mainly be attributed to economic and legitimacy considerations. The bottom line for China's data protection legislation is securing public security that is plainly anchoring at preserving the political status quo, namely, the ruling of the State. The strong commitment to public security may meanwhile provide a certain degree of protection of data privacy. But when such strong commitment turns to protect the political status quo (especially against political dissents or to implement mass surveillance), it poses serious threats to the data privacy of ordinary Chinese citizens.

The supremacy of public security against data privacy is observable from two aspects. First, a series of statutory and regulatory laws have legitimized government surveillance in the name of public security and cybersecurity. The Counterterrorism Law, for example, mandates telecommunication business operators and Internet service providers to offer technical support and assistance, including technical interface and decryption, to public security agencies for the purpose of preventing and investigating terrorist suspects.[106] The Counter-terrorism Law also empowers public security agencies to order Internet service providers to cease transmission and delete information containing terrorist or extremist content, and to shut down relevant websites.[107] Similar legal requirements can be found in the Criminal Procedural Law and the Counter-espionage Law.[108] Second, the legal restrictions on the exercise of investigatory powers of law enforcement agencies are symbolic to a large extent. The lack of meaningful legal control for public security agencies to collect personal data is probably intentional, because it could leave the Chinese government unfettered in the use of surveillance technologies, which have been proved to be a very effective regulatory tool for criminal investigation.[109]

The general empowerment of investigatory powers, combined with the lack of relevant meaningful legal control, tends to make ordinary citizens subject to excessive gov-

[104] 《人民法院民事裁判文书制作规范》 (The format of formulating a civil judgment by people's courts) Supreme People's Court, 2016.

[105] Hualing Fu, Susan Rose-Ackerman, and Paul Lagunes. "Wielding the sword: President Xi's new anti-corruption campaign." in *Rose-Ackerman, S & Lagunes P.* (Eds.) *Greed, corruption, and the modern state: essays in political economy* (Edward Elgar, London, 2015) pp. 157-158.

[106] See 《中华人民共和国刑事诉讼法》 (Criminal procedural law of the People's Republic of China) Article 149, and 《中华人民共和国反恐怖主义法》 (Counterterrorism law of the People's Republic of China) Article 45.

[107] The recent stringent control and mass surveillance measures taken in Xinjiang, to a large extent, go against the data subject's right to privacy protected under some Chinese law, see: Lily Kuo, Chinese surveillance company tracking 2.5 million Xinjiang residents, The Guardian, 18 February 2019, < https://www.theguardian.com/world/2019/feb/18/chinese-surveillance-company-tracking-25m-xinjiang-residents> Accessed 15 July 2020.

[108] See 《中华人民共和国刑事诉讼法》 (Criminal procedural law of the People's Republic of China) Article 149, and 《中华人民共和国反恐怖主义法》 (Counterterrorism law of the People's Republic of China) Article 45.

[109] For an extensive discussion on the application of network technologies in government surveillance in China, see Jyh An Lee and Chin Yi Liu, "Forbidden city enclosed by the great firewall: the law and power of Internet filtering in China", *Minnesota J Law Sci Technol* 13(2012), pp. 129-135.

ernment data mining and profiling.[110] Consistent with the fast expansion of digital economy, Chinese digital enterprises have gained considerable political and economic powers. As analyzed earlier, these digital enterprises are in a subordinate position to the State, and normally follow State's rules and policies to avoid further scrutiny. But they are also actively participating China's policy/law making processes. Digital enterprises have established their lobby groups and research institutes to influence policy/lawmaking as well as public opinions. By doing so, they have gained considerable trust and bargaining power. Economic interests are their dominating goal in corporate activities and they may risk a fight even with ministerial bodies of the central government given serious financial loss incurred due to the latter's regulatory activities. These digital enterprises may assist the State in conducting online surveillance and massive surveillance, but certainly do not dare to have a fight against government's requirements for (almost) unlimited access toto individual data collected by them.

Yet as already explained above, the escalating global criticisms of China's weak data and privacy protection regime may help these digital enterprises re-consider the issue. The growing global pressure (political, legal and economical) - especially from the US and the EU - may strongly motivate the Chinese government and major Chinese digital enterprises to make improvement, even superficial ones, in future data protection legislation and law implementation.

The awareness of ordinary Chinese on data privacy has been increasing. They demand more legal protection, mostly against aggressive data abuse of corporate powers, rather than against the Chinese government. Nevertheless, in a non-democratic country, which does not deem privacy as a fundamental human right, the public remains the weakest actor in the power relations. The unreasonable tradeoff between individual privacy and free service shows that the awareness of Chinese to data privacy is still low. As illustrated earlier, security and economic benefit are the major concern of digital companies, which highly overlaps with the Chinese state's law and policy agenda. The impetus to upgrade data privacy protection is growing, but not yet high enough to exert obvious influence on the future development of China's data protection law.

4.2. *Three possible paths ahead*

Although China plans to enact a comprehensive data protection law by 2022, what this law would finally look like remains unclear. By far, what we only know is that this law, as China's first comprehensive data protection law, would harmonize previously scattered laws and regulations, and is likely, to some extent, elevate the level of protection. The future is likely to see fierce contestation among the three key actors in the lawmaking arena. Given China's rapidly changing socio-economic landscape, it is too early to accurately predict the making of this Law. Notwithstanding the uncertainties, it is possible to identify the general directions of China's future data protection law by assessing different power relations among the three major actors. From this point of view, the future of China's data protection law is determined by how strong the support of data protection is from the three major actors in their future power dynamics. Accordingly, we predict that this future law may take one of three possible paths - the worst, the medium and the ideal.

The first possible but worst path is that China's future data protection law continues to uphold even stronger commitment to the supremacy of public security and economic development while take little account of data privacy protection. This may happen when political and economic crises arise. When facing the salutation that the crises (such as economic recession, financial crises or political unrest) threaten the political stability, the public security and economic growth would be prioritized and the value of data protection will be further marginalized. In case of conflicts between public security, economic development, and data privacy, the solution given by this Law is that the first two would certainly prevail over the latter. As a result, this Law will fail to provide any meaningful protection for data privacy. One the contrary, it would serve as a new instrument that facilitates and legalizes massive government surveillance and the excessive exploitation of personal data by technology enterprises. Thus, this Law only represents a new attempt of the Chinese government to gain legitimacy abroad while actually reinforce the legal and policy apparatus of ensuring public security and economic growth.

A good example of this worst type of law is the Law on Assembly, Procession and Demonstration (LAPD). Although claiming to "safeguarding citizen's rights to assembly, procession and demonstration" (Article One), this Law, in effect, deprives ordinary Chinese of these rights because most of the other thirty-five provisions contain restrictive or prohibitive rules against the exercise of these rights.[111] The violation of these restrictive rules might be determined as a criminal offence for disruption social order, which could be sentenced to imprisonment up to five years.[112] Given these severe restrictions, no formal application has been approved by public security agencies although unrest and protests have occurred frequently over the last three decades.[113] The LAPD is a radical case that shows how far a law meant for right protection could betray its claimed purpose in contemporary China. The LAPD has failed to achieve its said goal but has been very successful in achieving its hidden goal – eliminating any potential threats to public security. Upholding such hidden goal is understandable considering the unique circumstance when this Law was made - this Law was drafted in a very hasty manner

[110] Since China has neither meaningful check and balances nor judicial independence, the courts play no role in ensuring that administrative authorities will not abuse their powers during the collection and use of personal data, see Jyh-An Lee, "Hacking into China's cybersecurity law", *Wake Forest Law Rev* 53(2018), 101-102.

[111] See《中华人民共和国集会游行示威法》(The law on assembly, procession and demonstration) Standing Committee of the National People's Congress, Articles 8, 15, 21, 23-27.

[112] 《中华人民共和国刑法》(Criminal code of the People's Republic of China) National People's Congress, Articles 158 and 159.

[113] Xi Chen, *Social protest and contentious authoritarianism in China* (Cambridge University Press, New York, 2012), pp. 27-29.

and was adopted on 31 October 1989, four months after the end of the Tiananmen Square Protest.[114]

The first path is the worst among the three possible paths. The likelihood of China's future data protection law to follow this path should not be underestimated. First, new technologies have given the State unprecedented surveillance power ready for use. Big data has been deemed by Chinese government as an strategic asset relating to national security.[115] There have already been a range of existing laws and regulations that grant extensive power to the Chinese government to gain citizen's personal data. The State Council's ministries and committees in charge of public security and technology development would directly or indirectly create policy momentum that pushes the future legislation to follow the existing security-oriented legal regime. Second, the changing domestic and international security situation is also a factor that needs to be considered. A number of emerging security issues – frequent domestic unrests, the ongoing Hong Kong protests, Taiwan's Independent tendency, to name a few, have the potential to destabilize the country.[116] If a serious public security crisis outbreaks, the future Legislation on data protection is likely to follow the LAPD model. Moreover, once such a law was in place, it would have had long-term negative effect on the development of China's data protection as it would be difficult to return to the right path - the LAPD is one of a few national laws that have remained unchanged over the past three decades.

The second possible path is that while stressing public security and the development of digital economy, the proposed data protection law will provide more data privacy protection to individuals. Such a Law would represent some genuine efforts of Chinese lawmakers to enhance the level of data protection, but both its substantial contents and future enforcement may limit the final effect. This Law would be featured by the selective adoption of commonly recognized standards to fit the China's special circumstances. In other words, this Law is unlikely to incorporate all universal standards and principles that are commonly recognized in most countries' data protection law, let alone catching up with the newest law development led by the EU. In terms of enforcement, this Law is likely to be underused. Given the tolerable policy environment for government surveillance and economic development, the enforcement agencies ccould be reluctant to punish unreasonable data use by digital enterprises according to the strict data protection rules.

China has long been criticized for selective adoption of international standards in the name of preserving China's legal culture and safeguard State's interests.[117] For example, although China has ratified the International Covenant on Economic, Social and Cultural Rights, the legislative and policy-making practice has shown that China tends to prioritize the right to subsistence as the primary right and subordinate the protection of other civil and political rights.[118] There are ample evidences showing that China tends to adopt the selective approach to data protection legislation. For example, as one of the basic requirements in both the OECD Privacy Guideline and the Council of Europe Convention 108, data subjects' right of access to their personal data is missing in the 2016 Cybersecurity Law.[119] China's rights protection legislation generally faces implementation problems, which is already demonstrated by the enforcement of relevant laws on the protection of women, minors, elderly people and ethnic minorities. Take the legislation on ethnic minority protection as an example. The Law on the National Regional Autonomy has granted autonomous areas flexible powers, including the power to enact the comprehensive autonomous regulation. However, this power is seldom used - until now none of the five autonomous regions has enacted such regulations.[120] In the area of data protection, the weak enforcement of the existing legal rules is obvious. Resorting to civil remedies for addressing data abuse are not common. The enforcement of punitive rules in the Cybersecurity Law has been proved unsatisfactory since this Law went into effect on 1 June 2017.[121]

The second path for the development of data protection law is apparently better than the first path. Most likely the law development may move towards this direction for three major reasons. First the Chinese state still deems economic development as a cure-all solution, and therefore would provide considerable space for the development of data-driven economy. Thus, the State would choose to continue improving data protection for economic reason within the existing political ambit (not to threaten the Party's ruling). Second, China's corporate power, especially these large digital enterprises, will continue to grow and gain more political-societal voices in the near future, thus possibly pushing for a data protection regime

[114] Kam Wong, Law of assembly in the People's Republic of China, *Asia Pac J Human Rights Law 5 (2004), pp. 155-156.*

[115] 'Ł'Š'¿'ƒ'¿'›'¤'§'•'°'Ž'®'–"'±'•'¡'Œ'Š"'°'²'¡"'Ł'‹(Outline of action plan for promoting big data development) State Council, 2015.

[116] For the Hong Kong Protests in 2019, see: Daniel Victor and Alan Yuhas, What's happening in Hong Kong, New York Times, 8 August 2019, < https://www.nytimes.com/2019/08/08/world/asia/hong-kong-protests-explained.html> Accessed 20 July 2020; the Relationships cross the Taiwan Straits tends to be intensified as Taiwan plan to elect its new president in 2020, see: Tom Hancock, Nian Liu, China suspends individual tourist permits to Taiwan before election, 2019, Financial Times, <https://www.ft.com/content/6ba14934-b35e-11e9-8cb2-799a3a8cf37b> Accessed 20 July 2020.

[117] Pitman B. Potter, Legal reform in China: institutions, culture, and selective adaptation, law & social inquiry, 29 (2004), pp. 183-185.

[118] Pitman B. Potter, Selective adaptation and institutional capacity, perspectives on human rights in China, Int J 61(2) (2006) pp. 393-396.

[119] Graham Greenleaf, China's personal information standards: the long march to a privacy law, *privacy law & business Int Rep*, 150 (2017), pp. 25-28

[120] For an overview of the autonomous legislative power and the efforts to enact regional-level autonomous regulation, see Yash Ghai and Sophia Woodman, "Unused powers: contestation over autonomy legislation in the PRC", *Pac Aff* 82.1 (2009), pp. 38-41.

[121] 《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>实施情况的汇报》(Report on investigating the enforcement of the cybersecurity law of the People's Republic of China and the decision on strengthening information protection on networks) NPCSC Investigation Team, 2017.

that is more economy-oriented.[122] Third, although remaining an authoritative country, China has been generally becoming more liberal and tolerable since the Reform and Opening Up in 1978. Such general trends are irreversible in the long run, and are to be reflected in the development of data protection law. Notwithstanding the abovementioned benefits, the limitations of the second path are obvious. These positive changes in power relations and shifting value focuses won't go that far to treat data privacy as a fundamental right for constitutional protection against both State and corporate invasions. A modest data protection law is unlikely to assist the suppression of individual right to data privacy, but it is equally unable to overcome the above-mentioned problems plaguing China's data protection regime. China's future data protection law would fail to provide comprehensive and meaningful protection for Chinese citizens as it is expected. Therefore, this Law is most likely to have substantially elevating the level of data protection by laying out a basic regulatory framework with (barely) acceptable enforceability.

The third less possible, but most ideal path is that data privacy protection will gain considerable weight in China's future data protection law. This Law will not only incorporate basic requirements that are commonly found in other countries' data protection law, but also add new practical rules under the particular Chinese circumstances. The enhanced level of data protection could be reflected in two dimensions. On the one hand, the protection rules will apply to a wider areas of digital industries, and will cover more phrases of data processing. On the other hand, data subjects will be given more opportunities to control their personal data. More important is that this Law can provide meaningful protection against arbitrary data use by the government and digital enterprises. Data subject's access to judicial remedies will be guaranteed. By paying more attention to data privacy protection and holding both the government and digital companies accountable, this Law could better balance public security, economic development and individual rights protection.

From the perspective of rights protection, the third path for the development of data protection law is most desirable among the three possible paths. However, it should be noted that the primary goal of this Law is not for creating a model equivalent to that of the EU or the United States. Setting unrealistically high protection standards would be practically unenforceable at best, and cripple China's social stability and economic development at worst. Therefore, at this moment of time, the primary goal of the proposed law should be providing basic but meaningful protection for data privacy (with enforceability). This ideal path can only be taken under the following conditions. (1) Chinese State may become more liberal and gradually lean toward (human) rights protection to gain additional political legitimacy in addition to economic growth; (2) the rise of civil society can push for more privacy rights protection; (3) the private sector's aggressive approach to data use and profiling shall be constrained by an appropriate protection regime, which is jointly created by the State and the public.

5. Conclusion

The development of China's data protection law has come a long way and has been accelerated in recent years. It is very likely that a comprehensive data protection law will come into play by 2022. In any sense, the proposed Law will be forged via the dynamic and complex interactions between the State, digital enterprises, and the public. During this process, these actors will both collaborate and compete with each other in defending the three core values, namely, public security, economic development and individual privacy. The changing power relations of these three major actors in China's current political-legal context are decisive to the future of China's data protection law. Among the three possible paths, the second path is most likely to be adopted, although the third one is most preferable. However, the first (and worst probably) path is not impossible given that any sudden significant political, economic or security urgencies may emerge to alter the legislative directions.

Declaration of Competing Interest

None.

[122] The efforts of Chinese enterprises to promote data protection is similar to the US approach of a market-oriented legislation on data protection, See: Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the ground: driving corporate behavior in the United States* (The MIT Press, Cambridge, 2015), p. 49.