

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htmComputer Law
&
Security Review

The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams

Max Parasol *

China Law Research Group, University of Technology, Sydney, Australia
Lawyer and Law Lecturer, Monash University, Melbourne, Australia

ABSTRACT

Keywords:

China
Big data
The Internet of Things
Smart Cities
Network Sovereignty
Rule of Law
Cyber Security Laws

Chinese officials are increasingly turning to a policy known as Informatisation, connecting industry online, to utilise technology to improve efficiency and tackle economic developmental problems in China. However, various recent laws have made foreign technology firms uneasy about perceptions of Rule of Law in China. Will these new laws, under China's stated policy of "Network Sovereignty" ("网络主权" "wangluo zhuquan") affect China's ability to attract foreign technology firms, talent and importantly technology transfers? Will they slow China's technology and Smart City drive? This paper focuses on the question of whether international fears of China's new Cyber Security Law are justified. In Parts I and II, the paper analyses why China needs a cyber security regime. In Parts III and IV it examines the law itself.

© 2017 Max Parasol. Published by Elsevier Ltd. All rights reserved.

1. Introduction

In Part I, this paper provides background context by introducing China's Smart City drive. Smart Cities and associated technologies have deliberately been chosen for analysing China's Cyber Security Law for two reasons. Firstly Smart Cities must utilise all the technologies that China has officially stated are necessary for its development namely: the Internet of Things, cloud computing, big data and spatial geographic information systems. Big data informing these policy decisions is often collected from millions of smart devices, including mobile phones, that necessitate a cyber security regime.

Secondly Smart Cities can offset many of the political problems that besiege the Chinese Government and cause citizen unrest, namely air quality, traffic congestion, access to health-care and efficient government services. This intersection of incredibly complex policy decisions that keeps Chinese leaders awake at night, merits our direct attention.

China's Cyber Security Laws cannot be understood without understanding its Informatisation strategy. In Part II, this paper charts China's Informatisation Strategy and Network Sovereignty policies. This paper unpacks the Chinese policy statement that connecting industry online and cyber security are truly "two wings of one body". It is argued that the current Chinese Government values technological progress as China's key development task and accordingly recent controversial laws that worried foreign technology firms and governments were amended to avoid impeding technological goals, including China's 2015 Anti-Terrorism Law. In Parts III and IV, this paper objectively assesses China's Cyber Security Law at length. The law was passed by the National People's Congress on 7 November 2016, taking effect on 1 June 2017. While some provisions of this Law appear to tighten government control over Chinese and foreign technology firms, this paper presents evidence that suggests China will not harm its innovation agenda through excessive control over data and cyber technology.

* UTS Faculty of Law, University of Technology Sydney (UTS), City campus, 15 Broadway, Ultimo, NSW 2007, Australia.

E-mail address: maxparasol@rocketmail.com.

<http://dx.doi.org/10.1016/j.clsr.2017.05.022>

0267-3649/© 2017 Max Parasol. Published by Elsevier Ltd. All rights reserved.

There is a complete circle to be drawn. The Chinese Government must appease a population now expecting more from its leadership in terms of economic development and better quality of life while at the same time protecting them from cyber risks in an increasingly inter-connected world. These are complex policy considerations to balance.

To fulfil these demands, this paper contends that China must rely on assistance from both foreign and local technological innovators. These firms will therefore play a role in shaping the cyber security compliance debate in China. The text of the Cyber Security Law and subsequent regulatory developments allow for such negotiations over interpretation and enforcement. Negotiations may continue for another 18 months.

2. Part I: why China needs a Cyber Security Regime

The following background is necessary to understand why China needs a cyber security regime, especially in relation to China's national policy of using the internet and big data to resolve long-standing development problems.

The enactment of the Cyber Security Law in 2016 arguably reflected more than a legislative attempt to regulate the internet for the purpose of censorship. The law was passed by the National People's Congress on 7 November 2016, but did not take effect until 1 June 2017. There have been a number of attempts to lobby the Cyberspace Administration of China (CAC)¹ to delay implementation. On 15 May 2017, global technology companies represented by 54 trade groups from Europe, Asia and the US petitioned China to delay the enactment of the Cyber Security Law.² Their major argument is that it could discriminate against foreign businesses. This paper argues that China will continue the ongoing compliance debate with foreign technology companies and that reports of CAC "[i]ndiscriminately requiring businesses to hand over source codes" are inaccurate.³

2.1. Billions of connected devices

The Cyber Security Law was a necessity for Smart Cities and associated technologies to develop in a safe and secure way. China has 731 million internet users according to government statistics in January 2017. Further, 695 million users use the internet through mobile devices. They rarely use cash and rely on

China's distinct online, e-commerce, payment and logistics ecosystem.⁴

Cyber technologies will define the 21st century. Cyber security must therefore be part of everything that we create. While this can be linked to national and global security, it is also through this lens that fears surrounding China's Cyber Security Law can be reduced. As Smart Cities utilise key public infrastructure, a close reading of China's new Cyber Security Law indicates that cyber security concerns focused on "critical infrastructure" were a primary policy driver for the new law.

The Chinese Government has focused its attention on an innovation agenda, and that may be hard for the international community to grasp. Observers must look for the intent behind the law from the wider Chinese policy context, and the massive task of ensuring network security among China's billions of connected devices.⁵

2.2. China's history of legislative petri dishes

There are over 300 Smart City pilot projects⁶ across China. They build upon China's history of what I call 'law in a petri dish', or the legislative laboratory that China has created since 1978 in China's Special Economic Zones and Technology Development Zones.⁷ These national level programs started with the Special Economic Zones for three cities in 1978, as part of China's economic reform, and were extended to the Economic and Technological Development Zones in 14 cities in 1984. The phrase "Special Economic Zone" itself belies their role in Chinese law and development history. They evolved as a place for political and economic policy experimentation.

Wei-Wei Zhang in *Transforming China: Economic Reform and its Political Implications* sums up the experimental role of the Special Economic Zones:

The SEZs became, effectively, laboratories in which the operation of the market economy was carried out. The intention of the state was to extend methods that proved successful in the zones to other parts of the country. Should the experiment fail, its adverse impact could be minimized since the zones were located far away from China's political and economic centres. The strategy was

¹ Discussed in detail below, CAC is the office that outlines China's cyber strategy.

² The letter was signed by 54 trade groups including the US-China Business Council, American Chamber of Commerce in China, BusinessEurope, the Japan Chamber of Commerce and Industry and the Korea-China Business Council. see: Eva Dou, 'Global Tech Companies Call on China to Delay Cybersecurity Law', (*Wall Street Journal*, 15 May 2017) <<https://www.wsj.com/articles/global-tech-companies-call-on-china-to-delay-cybersecurity-law-1494837117>> accessed 18 May 2017.

³ Michael Martina and Cate Cadell, 'Amid industry pushback, China offers changes to cyber rules: sources' (*Reuters*, 19 May 2017) <<http://www.reuters.com/article/us-china-cyber-law-idUSKCN18F1VZ>> accessed 21 May 2017.

⁴ This is according to Chinese Government statistics released in January 2017. See: Steven Millward, 'China now has 731 million internet users, 95% access from their phones', (*TechinAsia*, 23 January 2017) <<https://www.techinasia.com/china-731-million-internet-users-end-2016>> accessed 23 January 2017.

⁵ China has been predicted to have 10 billion connected devices by 2020. Mary Lennighan, 'China to have 10bn connected devices by 2020', (*Total Telecom*, 24 February 16), <<https://www.totaltele.com/view.aspx?ID=492917>> accessed 25 March 2017.

⁶ At present, there are more than 300 pilot Smart Cities in China. 'Sector Report: Smart Cities in China' (2016) EU SME Centre, <http://www.cbcc.org/cbbc/media/cbbc_media/KnowledgeLibrary/Reports/EU-SME-Centre-Report-Smart-Cities-in-China-Jan-2016.pdf> accessed January 2017, p20.

⁷ The Chinese Government allowed two provinces of the four provinces, Shenzhen in Guangdong Province and Xiamen, Fujian Province, to adopt "special policies" (*teshu zhengce* 特殊政策) and to implement "flexible measures" (*linghuo cuoshi* 灵活措施). These unique powers were aimed at attracting foreign capital and technology. They were granted preferential tax measures and enjoyed higher foreign-exchange retention rates.

Download English Version:

<https://daneshyari.com/en/article/6890596>

Download Persian Version:

<https://daneshyari.com/article/6890596>

[Daneshyari.com](https://daneshyari.com)