Unpacking China's Social Credit System: Informatization, Regulatory Framework, and Market Dynamics

Lianrui Jia
York University

ABSTRACT

Background *China, with a population of 802 million internet users, a handful of the world's largest internet companies, and an unfolding Social Credit System (SCS), is often criticized for exerting its data power to surveil and discipline its population.*

Analysis *This article first provides a historical and situated analysis of the SCS as a part of China's informatization and datafication processes. It then highlights problems in the current legal and regulatory data-protection framework and discusses the self-regulation practices of the private sector.*

Conclusions and implications *Overall, this case study provides a historical and contextualized understanding of China's SCS and related big data developments and assesses the implications of these development for the globalizing Chinese internet, technology companies and the Chinese public.*

Keywords *China; Big data; Social credit system; Chinese internet*

RÉSUMÉ

Contexte *Avec une population de 802 million d'utilisateurs d'Internet, avec quelques des plus grandes sociétés Internet du monde, et une Système de Crédit Sociale (SCS) en pleine développement, La Chine est souvent critiqué pour utilizer son pouvoir de données pour surveiller et discipliner sa population.*

Analyse *Tout d'abord, cet article fournit une analyse historique et située de la SCS comme partie des processus de informatisation et datafication de la Chine. Ensuite, il souligne les problèmes du cadre juridique et régulatoire actuel en matière de protection des données et examine les pratiques d'autorégulation du secteur privé.*

Conclusions et implications *En global, cette étude de cas fournit une compréhension historique et contextualisée du SCS chinois et de l'évolution du Big Data, et évalue les implications de ce développement pour l'Internet chinois en pleine mondialisation, les entreprises technologiques et le public chinois.*

Mots clés *La Chine; Big data; Système de Crédit Sociale; l'Internet chinois*

Lianrui Jia is a doctoral candidate in Communication and Culture at York University, 3006 Victor Philip Dahdaleh Building, York University, 4700 Keele Street, Toronto, Ontario M3J 1P3. Email: lianrui.jia@gmail.com .

Canadian Journal of Communication Vol 45 (2020) 113–127 ©2020 Canadian Journal of Communication Corporation http://doi.org/10.22230/cjc.2020v45n1a3483

Introduction

The quick rate of China's internet development has simultaneously impressed the world and alerted it to China's data power (see, for example, Mistreanu, 2018). With the first internet connection established in 1987, China's internet growth has been substantial: China now has an internet population of 802 million and a penetration rate of 57.7 percent (CNNIC, 2018). The sheer size of the online population and its computational power make it a lucrative market and a business destination, but it has also become a place with a treasure trove of data—data of geopolitical and economic importance. With the convenience of each mobile phone as tracker, sensor, and surveyor, Chinese society is quickly being datafied at the behest of state and corporate interests. This article focuses on one of the most significant moves toward the national deployment of big data in China: the Social Credit System (SCS). It asks three key questions: What is the developmental trajectory and historical context of China's SCS? What is the legal and institutional framework that guides and supervises these big data developments? What are the social implications of this technical assemblage within the current context of Chinese commercial internet development? Using political economy as the underlying theoretical framework of analysis, this article contributes to a historically informed understanding of China's SCS, focusing on the articulation and arrangements of power between the Chinese government, emerging commercial internet companies, and society.

Social Credit System

Instituted in 2014 by the State Council in the Plan for the Construction of the Social Credit System (SCS) (State Council, 2014), China's SCS is a national project that sets a comprehensive outline for the establishment of data infrastructure for credit scoring. To be completed by year 2020, the SCS also offers a reward and punishment system in all areas of social life and for all walks of life, including government affairs, judicial affairs, and social activities (Meissner, 2017). The meaning of "credit" in the SCS is expansive, including both financial credit and trustworthiness defined in the 2007 State Council's Guiding Opinions Concerning the Constructions of a Social Credit System, to trust and honest conduct in the Planning Outline for the Construction of a Social Credit System in 2014 (Creemers, 2018; Liang, Das, Kostyuk, & Hussian, 2018). The blueprint of the 2014 SCS projects a nationwide system, a major upgrade in scope and scale from various existing municipal- or city-level social credit system pilots, such as Honest Shanghai and Honest Hangzhou, to realize the goal of social management (Creemers, 2018) and steering social behaviour changes (Kostka, 2019). The Social Credit System also includes various reward and punishment schemes (e.g., the creation of red and blacklist), with the goal to solve the deep-seated problems that plague China's legal reform—ensuring effective legal and regulatory implementation, enforcement, and compliance for issues such as food safety and environmental regulation (Creemers, 2018; Kostka, 2019).

Given the unprecedented scope and scale of the SCS, a slew of academic studies have examined the nuts and bolts of the system. Legal scholar Xin Dai (2018) considers the SCS to be part of a larger transformation toward the reputation state, where reputation-based decision-making creates behavioural incentives for social actors of a par-

ticular group. While others see China's SCS as the epitome of data-driven governance, which harnesses surveillance as a tool to shape and create social worlds (Backer, 2018). Compared to the "scored society" conceptualized by Danielle Citron and Frank Pasquale (2014), where the pervasive use of predictive algorithms is deployed to mine personal information to make guesses about individual's likely actions and risks, the SCS engages government as well as private actors, not so much for risk reduction but to engage social engineering for the purpose of social governance and management in sync with China's deepening market reform (State Council, 2014). As China lacks a well-established credit rating and credit card industry (Xu, Tang, & Guttman, 2019), the demand for a credit system dated back to malicious accounting and loan-lending activities that prevailed during the market reform era of the 1990s (Liang et al., 2018). Overall, the significance of the current SCS construct, as Fan and his colleagues argue (2018), goes beyond the monitoring of the day-to-day activities of average citizens to the buildup of a nationwide surveillance infrastructure that upgrades the government's ability to surveil all facets of society and normalizes a broader culture of surveillance via the "infrastructurization" (p. 17) of platforms.

Contrary to many dystopic depictions of the SCS, research study finds, through a large-scale survey, that there is a very high level of public support for the SCS and virtually no disapproval, in particular among the better-educated and wealthier population and those who receive the actual reward benefit (Kostka, 2019). Public support for local government SCS pilots is high (Kostka, 2019), which complements previous studies on public concerns over commercial credit systems such as Sesame Credit, where users expressed a lack of understanding of how the black box worked (Ahmed, 2017b).

These studies shed light on the inner workings of the unfolding SCS, its historical origins (Liang et al., 2018), potential obstacles for implementation (Dai, 2018; Liang et al., 2018), and the implications it may have for existing laws and regulations and society writ large (Backer, 2018; Creemers, 2018). Although the SCS sets out ambitious plans, scholars are cautious in projecting its actual implementation. Implementation requires expansive institutional support, cultural legitimation, and legal safeguards. Current ongoing SCS experiments are taking shape in various parts of China in accordance with specific socio-technical conditions. In Rongcheng, for example, a city at the forefront of China's SCS movement, the maintenance and operation of the system hinges upon a group of 10 information gatherers; they use piles of paper and pens to record every instance of voluntary work and every donation fellow residents give to the community, in order to account for the rewards and punishment they should receive (Gan, 2019). In 2017, China's Supreme People's Court reported 6.15 million Chinese citizens had been banned from taking flights for social misdeeds (Reuters, 2018a). By the end of 2018, Chinese courts banned would-be travellers from buying flights 17.5 million times (Kuo, 2019). In no small way, the governance power of SCS is real and looming. Beyond impacts felt by the individual, the SCS also serves a larger purpose in transforming how the state governs and makes policy decisions, which draws historical parallels to the Golden Projects that were instituted in China in the 1990s. The next section traces the connections and distinctions between these two projects to contextualize the significance of the SCS.

China's informatization: From Golden Projects to the Social Credit System

Chinese big data development can be regarded as the latest iteration of the state's informatization strategy, which was adopted in the 1980s to build an "information society" (Jiang & Fu, 2018). In the late 1970s, China embarked on informatization as part of the national strategy to modernize and achieve the transition from an agricultural, central planning society to an industrial society with a socialist market economy. Under the banner of informatization, the Chinese government supported the research and development of new technologies with the hope of leapfrogging development into a post-industrial economy, following Alvin Toffler's (1980) prophecy in *The Third Wave.* Within the past three decades, China not only rapidly wired the country and reformed its telecommunication industry (Harwit, 2008), it also successfully fostered and assembled a team of commercially successful national champions (e.g., Huawei, Lenovo, and ZTE) (Eaton, 2015). Furthermore, a series of e-government initiatives called Golden Projects was put in place to spearhead the informatization of government administration and management. Table 1 lists the key components of the Golden Projects. The first twelve were pilot projects led to the construction of the infrastructure for China's e-government procedures, as stipulated by *State Council Document No. 17* in 2002 (Liang, 2006). Most of these projects operated on the e-government internal network, directly linking to main databases.

The Golden Projects were implemented to achieve three main objectives: to strengthen government supervision and efficiency, to safeguard government revenue and rationalize government spending, and to ensure basic order in the national economy and social development (Liang, 2006). Probably one of the most notorious projects was the Golden Shield Project, later known as the Great Firewall, developed by the Ministry of Public Security with help from companies such as Nortel, Sun Microsystems, and Cisco. A project called the Golden Card Project, personally initiated by then-President Jiang Zemin, promoted the usage of credit and cash cards; it also prompted the inter-linking of automated teller machines (ATMs) between five major Chinese banks: Industrial Bank, Agricultural Bank, Bank of China, Construction Bank, and Communications Bank (Dai, 2000).

Table 1: Golden Projects overview

	Project title	Project description
1	Golden Bridge	Building an information superhighway to promote commercial internet service
2	Golden Custom (Golden Gate)	Project linking customs points through national electronic data exchange for foreign trades
3	Golden Card	Promoting the use of electronic currencies, credit card, and radio-frequency identification (RFID) technology
4	Golden Tax	Using information technology to crack down on tax evasion

Table 1 (continued)

	Project title	Project description
5	Golden Finance	Establishing a clearing house for financial management
6	Golden Audit	Establishing a centrally organized electronic auditing system for government entities
7	Golden Social Security	Unified national information system for labour protection and social security
8	Golden Quality	Building a standardized national network for quality supervision
9	Golden Marco	Macroeconomic management information system
10	Golden Agriculture	Information exchange network for agriculture production, market supervision, and an animal disease-warning system
11	Golden Water	Basic infrastructures for data-sharing for water conservancy
12	Golden Shield	National public security work information project
13	Golden Travel	Establish an information network and management system to oversee tourism services
14	Golden Hygiene	Medical information network
15	Golden Education	Electronic network for public education and administration
16	Golden Trade	Electronic network for e-commerce and trade for China's participation in the global market

Sources: Author's compilations; Dai, 2000; Liang, 2006

As Xi Jinping came into power, informatization assumed a renewed strategic importance, especially under the political and economic realities of the time: informatization aims to provide a new engine and productive force for sluggish economic development and secure and enhance China's aspiration of becoming a cyber superpower. Xi remarked on the first meeting of the Cybersecurity and Informatization Leading Small Group in 2014: "there is no national security without cybersecurity; there is no modernization without informatization" (Elsa, Sacks, Triolo, & Webster, 2017), reaffirming the crucial role internet and information and communications technology (ICT) are set to play in national development. The state government was also quick to realize the uses of big data and became an avid advocate for its potential in a series of government initiatives. Tencent (2017) CEO Ma Huateng first proposed the "Internet Plus" concept in 2013, and it was later endorsed and promoted by Premier Li Keqiang in 2015 in the *Government Work Report* as top-level strategy. The Internet Plus plan enacted mobile internet, cloud computing, big data, and the internet of things to upgrade traditional industries and create new poles of economic growth (Xinhua, 2015). In the Thirteenth Five-year Plan, big data was elevated into a national strategy and a crucial strategic resource to help upgrade industrial reform and social governance.

Overall, big data development in China largely followed the emerging big data ideology that legitimated the continuous and large-scale extraction and processing of data as the basis of constructing a "brave new world" (Couldry & Yu, 2018), propelled by both the government's appetite to better grip and exert control over the commercial motives of private corporations (Ahmed & Weber, 2018; Creemers, 2017).

In the same year, the State Council put out a comprehensive blueprint for the SCS. The plan set out four focused areas for the construction of the credit system (see Table 2). Compared to the Golden Projects, the SCS provided a much more unified and systematic upgrade to informatization, which had been underway since the early 1990s. The grounds covered by SCS were much more expansive and centralized. Most importantly, the SCS launched a reward and punishment scheme to tackle the "implementation problem" (Creemers, 2018). The Golden Projects digitized and informatized government services and management in preparation for China's accession into the World Trade Organization (WTO), while the SCS incorporated society as a whole and fostered education and moral guidance (Backer, 2018; Creemers, 2018). Nonetheless, both systems were similarly framed in a technocratic and "techno-solutionist" tone that regarded ICTs as the panacea of the social problems that emerged during China's market reform (Jiang & Fu, 2018). The system embarked upon and unleashed the normalization of datafication as a new paradigm for Chinese society, allowing for default data collection about daily activities to provide legitimate access to, understand, and monitor people's behaviour (van Dijck, 2014). Furthermore, big data development was wrapped in China's techno-nationalism (Feigenbaum, 2017) and cyber superpower ambition, which considers success in a high-tech race essential for building national pride and national power. Framing high-tech development as a global competition that China cannot afford to lose, a discourse of technological nationalism tied social media and big data to China's overall informatization and modernization by tapping into a deep swell of Chinese national pride (Jiang & Fu, 2018).

Table 2: Social Credit System design

Focused areas	Sub-areas
Government affairs	Administrative permission, government procurement, labour and employment, social security, cadre promotion and appointment, management, government performance
Commercial activities	Safety and quality control in manufacturing production, credit rating and assessment, financial credit system, tax, pricing, project construction, government procurement, tendering and bidding, transportation, e-commerce, statistics, advertising and exhibitions, enterprise management
Social activities	Medical and healthcare, social welfare, labour market, education and research, cultural, tourism and sports, intellectual property, environment protection, social organization, occupation certification, internet application and service
Judicial	Transparency in proceedings, prosecutorial credibility, public accountability, public security, judicial administrative systems, law enforcement standardization

Source: State Council, 2014

Regulatory framework

This extensive and concerted effort to gather and analyze data to reward or punish behaviours, and with the success of the SCS (Backer, 2018), required the simultaneous development of laws for the digital and data age. It was imperative to operate a data system to protect the integrity of the generation of data. Since 2012, the Chinese government has stepped up its effort in building a robust data protection regime (see Table 3) (Sacks, Shi, & Webster, 2019). Pressures were tabled at the top legislature in the Standing Committee of the National People's Congress about the urgency to establish a systematic legal regime to protect privacy and personal information to keep pace with tech and big data development.

Table 3: Chinese data protection framework (2019)

Year	Title	Government ministries	Legal effect
2010	Tort Liabilities Law	Standing Committee of the National People's Congress	Civil Law
2012	Decision on Strengthening Online Personal Data Protection	Standing Committee of the National People's Congress	General Framework
2013	Telecommunication and Internet User Personal Data Protection Regulations	Ministry of Industry and Information Technology	Department Regulation
2013	Information Security Technology Guidelines for Personal Information Protection with Public and Commercial Services Information Systems	National Information Security Standardization Technical Committee; China Software Testing Center	Voluntary National Standard
2015	Criminal Law (9th Amendment)	Standing Committee of the National People's Congress	Criminal Law
2017	Cybersecurity Law	Standing Committee of the National People's Congress	Law
2018	Personal Information Protection Standard	Standardization Administration of China	Voluntary National Standard
2018	E-Commerce Law	Standing Committee of the National People's Congress	Law
2019	Personal Information Protection Standard	Drafting	
2019	Measures for Data Security Management	Drafting	

Sources: Author's compilation; Sacks, Shi, & Webster, 2019

Several observations can be made about this recent raft of regulations: first, current regulatory authorities regarding privacy and data protection are dispersed across many government agencies and in various laws (e.g., criminal and civil law), rulings, and national standards. Although these efforts did establish a systematic legal and regulatory data protection regime that was largely absent, problems with interpretation and enforcement prevail. On one hand, national standards are only voluntary mea-

surements and do not require legal compliance. On the other hand, the Cybersecurity Law contains contradictions, such as Article 24, which stipulates real-name registration policies and demands network operators to obtain usernames and personal information when registering for services (Lee, 2017). As the law provided citizens with unprecedented protection for their data, it also created numerous opportunities for the government or third parties to infringe upon citizen's privacy (Lee, 2017). Furthermore, there are inconsistence between national standards and the Cybersecurity Law regarding the definition of consent, thus leaving space for interpretation by enforcement authorities (Sacks, 2018). These contradictions challenged the coherence of the data protection regime and tarnished the high standard of protection warranted by the Cybersecurity Law (Greenleaf & Livingston, 2017).

Second, regulations tended to emphasize the importance of data protection for the ends of national security and economic development rather than individual concerns of privacy. A prominent example was the adoption of the category of "important data" in the Cybersecurity Law Article 31, which are data that, if leaked, might endanger national security, national welfare, and public interest (Wangluo Chuanbo Zazhi, 2017). Existing Chinese laws and regulations tilted toward the protection of national security over individual rights. This fits with the larger trend within Chinese internet regulation and law-making processes where economic protectionism is often fused with national security, further obscuring the line between them as China sets out to reduce dependency on foreign technologies (Ahmed & Weber, 2018). In general, online privacy enjoys only a modicum of legislative protection in China (Wu, Lau, Atkin, & Lin, 2011).

Outside the purview of national laws and regulation, industry self-regulation regarding data protection are also emerging. The Internet Society of China (ISC) established the Personal Information Protection Committee in 2017, reaffirming the prevalence of privacy infringement and the urgent need for protection (ISC, 2017). In the 2016 *Chinese Internet User Right Protection Report* issued by the ISC (2017), 76 percent of internet users received fraudulent phone calls and messages from banks, internet companies, and television stations, and 54 percent of internet users think personal information leakage is very serious while 84 percent have been personally affected by such leakage. Government-enlisted companies in nationwide big data projects—such as Baidu, Alibaba, and Tencent—proved to have a bad record of data protection. Alibaba's payment service, Alipay, was scrutinized by the Cyberspace Administration of China for enrolling users into its credit scoring system, Sesame Credit, without gaining user consent (Reuters, 2018b). The Ministry of Industry and Information Technology (MIIT) investigated Baidu and Tencent over poor privacy protection practices, for lacking proper and clear notifications for the collection and use of personal information. In the report by Ranking Digital Rights (2017) on the corporate accountability index, which measures governance, freedom of expression, and privacy, Baidu and Tencent scored poorly compared to other global internet companies, ranking 10 and 12 among the 12 internet and mobile companies examined.

Overall, domestic Chinese internet companies' data protection measures and practices were scant and inefficient. Together with the Chinese University of Political Science and Law, the *Southern Metropolis* (2017) newspaper tested 1,000 Chinese Web

services and mobile applications. The study found that no company reached a "high" standard of transparency in terms of a privacy policy and nearly 80 percent of services ranked "low" and "very low." Data breaches and leaks are a common occurrence for average internet users in China (Southern Metropolis, 2017). On the four-hundredth day of the enactment of the Cybersecurity Law, the same test was conducted on 100 popular applications and results showed that although the level of transparency for privacy policies improved, 13 applications still had no privacy policies (Southern Metropolis, 2018). Also, internet intermediaries are largely self-regulated when it comes to data protection, which means there are hardly any standard practices for obtaining user consent. Enterprises identify the lack of privacy protection as the biggest obstacle for the application of big data technologies (CAICT, 2018). Research revealed, for example, that the country's most popular mobile chat application, WeChat, installs filters for tracking for both texts and images under the pressure of state regulation to closely monitor online communication (Knockel, Ruan, Crete-Nishihata, & Deibert, 2018), even though its parent company, Tencent, publicly claims that user data security is a top company concern (Chen & Deng, 2018). Furthermore, lacking judicial independence and effective checks and balances, individual users cannot claim any remedies for the infringement on their privacy carried out by the state government (Lee, 2017). For instance, Chinese journalist Liu Hu who writes about censorship and government corruption was arrested, fined, and blacklisted on the Dishonest Persons Subject to Enforcement by the Supreme People's Court, but because of his work and the lack of files, police warrant, or official notification, Liu found nowhere to complain or report to (Kobie, 2019).

In 2017, Baidu's CEO, Yanhong Li, made a comment that angered many Chinese netizens: "If they (Chinese internet users) can trade privacy for convenience, for security, for efficiency, in a lot of cases, they are willing to abide" (Global Times, 2018). Former Google China president Kai-Fu Lee made a similar comment, "Chinese users are willing to trade their personal privacy data for convenience or safety. It's not an explicit process but it's a cultural element" (Webster & Kim, 2018). Even though privacy is perceived differently by Chinese society as compared to the West, and sometime carries a negative light given the socio-cultural context, there is an awakening and a sensitivity to state surveillance and the intrusion of commercial interests into individual privacy among Chinese internet users (Yuan, Feng, & Danowski, 2013).

Market dynamics

It is in the political and economic interest of the Chinese government to secure and build a strong domestic internet industry and to foster globally competitive Chinese internet platform companies. Prior to the SCS, domestic internet companies, represented by the BAT (Baidu, Alibaba, and Tencent) already held much sway in China's internet governance agenda, on the global stage (Shen, 2016), in the domestic policy arena (Hong, 2017a), and in helping state economic transition and progress (Hong, 2017b). Alibaba and Tencent, for example, assisted local police in the Smart City project by providing surveillance networks and a cloud-based data system to facially recognize and arrest criminals and to track and forecast the movement of crowds (Lin & Chin, 2017). The SCS further fosters a symbiosis between the state and leading Chinese

platform companies (Ahmed, 2017a; Jia, 2018; Jiang & Fu, 2018). In the construction of SCS, private Chinese platform companies were assigned an important role. The government handpicked five technology companies to co-develop an artificial intelligence open-innovation platform: Baidu for self-driving cars, Alibaba for the smart city, Tencent for medical imaging, and iFlyTek for voice recognition (Xinhua News Agency, 2017).

However, the symbiosis between the state and leading Chinese platform companies is by no means given and uncontested. In 2015, People's Bank of China (PBOC) selected eight companies to pilot a unified personal credit platform for online lending. An episode in the tug-of-war between the PBOC and technology companies further illustrated the tensions and problems that arise when big technology companies take over government functions in big data development. The PBOC issued a notice giving each technology company six months to prepare (State Council, 2015). However, in the Personal Information Protection and Credit Management Forum held in 2017, PBOC Credit Bureau Chief Wan Cunzhi said that none of these eight tech firms met the licensing criteria, and questioned their ability to build full-fledged credit bureaus (Cadell & Zhang, 2017). The PBOC worried about the technology companies' independence, whether those eight tech companies could meet the public's expectation for privacy protection, and the conflict of interests between these companies as they each occupied a business segment and were not willing to share collected information (Shanghai Securities News, 2017). The PBOC was well aware that the ultimate interest of Tencent and Alibaba is in the sale of products, not public service (Hornby, Ju, & Lucas, 2018). The final institutional set up of the unified personal credit platform for online lending was later spearheaded by the National Internet Finance Association, which controls the majority stake of 36 percent of the platform; each of the eight companies holds an eight percent stake (China.org, 2018). In the meantime, the state has tightened online finance regulation—Tencent's credit-scoring agency only survived for one day after its launch and then it was shut down by the Central Bank (Bloomberg, 2018).

Globally speaking, as Chinese internet and ICT companies expanded overseas, surveillance became a lucrative business segment in which Chinese companies rapidly established a market presence. Under the auspices of China's Belt and Road Initiative, the Zimbabwe government signed a strategic partnership with a Guangzhou-based startup CloudWalk Technology to build a large-scale facial recognition program throughout the country, covering CCTV cameras, smart financial systems, airports, and railway and bus station security (Chutel, 2018; Hawkins, 2018). ZTE also assisted the Venezuelan government to develop a "fatherland card" and database, and to create a mobile payment system, raising concerns over the possible misuse of the information to stifle political opponents (Berwick, 2018). ZTE also provided the infrastructure for the Ethiopian government (Maasho, 2013). Huawei's "safe city" solutions were also installed in more than 100 countries, from Serbia to Mauritius, and the company took part in the "safe Philippines" deal during Xi Jinping's visit to the country, installing 12,000 closed circuit television cameras in Manila (Mandhana, 2019). Aided by the Chinese state, Chinese internet and technology enterprises also export the tools and

equipment that operationalize the Chinese model of internet control and its internet sovereignty governance model, which favours the role of the state over the rights of netizens.

Conclusion

In probing open data initiatives in the Global South, such as India's biometric identity project, Payal Arora (2016) warns that we must recognize that these databased techniques of democracy are assemblages of institutions, policies, histories, cultural practices, and situational contexts that play out in a complex unison to materialize and articulate the plural realities of governance. This statement sheds important light on the SCS in China and how this system developed out of the distinctive informatization path led by the Central Communist Party to modernize the nation since the 1970s and the renewed national aspiration to become a global cyber superpower under the leadership of Xi Jinping. The implementation of the SCS is closely knitted with the sociotechnical conditions and realities of Chinese society, where in 2018, internet penetration is slightly more than half of the country's population (55.8%), of which only 27 percent are rural populations (CNNIC, 2018). To what degree the SCS will enlarge or close the rural-urban gap that plagued the historical development of Chinese telecommunication and internet (Hong, 2017b; Zhao, 2000) should be closely examined, especially as urban populations have access to more of the offered rewards (Kostka, 2019). Recent incidents have already demonstrated that ethnic minorities are prone and vulnerable to perilous data leaks, such as the facial recognition databases tracking the Uyghur Muslim population (Cimpanu, 2019). Furthermore, as the Chinese government gradually catches up on establishing a robust data protection regime to provide the necessary legal safeguard to the domestic development of the SCS, it will have long-standing implications for globalizing Chinese internet platform companies as they export goods and services to other nations and markets. To be certain, conflicts and contentions loom ahead between increasing public awareness for privacy protection (Soo, 2018), the business model of internet platform companies that hinge on ever more expansive data collection and the political interest of predicting and preempting individuals and movements that might be seen to endanger social stability.

Acknowledgement

The author wishes to thank Dr. Tracey Lauriault, Dr. Merlyna Lim, and the two anonymous reviewers for their comments on this article.

References

Ahmed, Shazeda. (2017a). Cashless society, cached data. *The Citizen Lab*. URL: https://citizenlab.ca/2017/01/cashless-society-cached-data-security-considerations-chinese-social-credit-system/ [January 24, 2017].

Ahmed, Shazeda. (2017b). Consumer protection oversights in the Chinese Social Credit System. *Digital Credit Observatory*. URL: http://www.digitalcreditobservatory.org/consumer-protection-oversights-in-the-chinese-social-credit-system.html [July 5, 2017].

Ahmed, Shazeda, & Weber, Steven. (2018). China's long game in techno-nationalism. *First Monday*, *23*(5). doi: 10.5210/fm.v23i5.8085

Arora, Payal. (2016). The bottom of the data pyramid: Big data and the Global South. *International Journal of Communication*, *10*, 1681–1699.

Backer, Larry Catá. (2018). *Next generation law: Data driven governance and accountability based regulatory systems in the West, and Social Credit Regimes in China.* URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3209997 [July 30, 2018].

Berwick, Angus. (2018). How ZTE helps Venezuela create China-style social control. *Reuters.* URL: https://www.reuters.com/investigates/special-report/venezuela-zte/ [November 14, 2018].

Bloomberg. (2018). Where China's tech giants may face the limitations of innovation. *Bloomberg.* URL: https://www.scmp.com/business/china-business/article/2133197/where-chinas-tech-giants-may-face-limitations-innovation [Feburary 13, 2018].

Cadell, Cate, & Zhang, Shu. (2017). No more loan rangers? Beijing's waning support for private credit scores. *Reuters.* URL: https://www.reuters.com/article/ant-financial-credit/no-more-loan-rangers-beijings-waning-support-for-private-credit-scores-idUSL3N1JO05W [July 4, 2017].

CAICT. (2018). Zhongguo Dashuju Fazhan Diaocha Baogao. *CAICT.* URL: http://www.caict.ac.cn/kxyj/qwfb/ztbg/201804/P020180426332651074674.pdf [April 18, 2018].

Chen, Celia, & Deng, Iris. (2018). Tencent says it will comply with law enforcement requests on user data. *South China Morning Post.* URL: https://www.scmp.com/tech/social-gadgets/article/2138249/tencent-profit-doubles-strong-smartphone-games-business [July 20, 2018].

China.org. (2018). China to launch 1st unified personal credit platform for online lending. *China.org.* URL: http://www.china.org.cn/business/2018-01/05/content_50191751.htm [Janurary 5, 2018].

Chutel, Lynsey. (2018). China is exporting facial recognition software to Africa, expanding its vast database. *QuartzAfrica.* URL: https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/ [May 25, 2018].

Cimpanu, Catalin. (2019). Chinese company leaves Muslim-tracking facial recognition database exposed online. *ZDNet.* URL: https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/ [Feburary 14, 2019].

Citron, Danielle, & Pasquale, Frank. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, *89*(1), 1–33.

CNNIC. (2018). Statistical report on internet development in China. *China Internet Network Information Center.* URL: https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf [July 30, 2018].

Couldry, Nick, & Yu, Jun. (2018). Deconstructing datafication's brave New World. *New Media and Society,* 20(12), 4473–4491. doi: 10.1177/1461444818775968

Creemers, Rogier. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China*, *26*(103), 85–100. doi: 10.1080/10670564.2016.1206281

Creemers, Rogier. (2018). China's Social Credit System: An evolving practice of control. *SSRN.* URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 [May 22, 2018].

Dai, Xin. (2018). Toward a reputation state: The Social Credit System project of China. *SSRN.* URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193577 [June 24, 2018].

Dai, Xiudian. (2000). *The digital revolution and governance.* Farnham, UK: Ashgate.

Eaton, Sarah. (2015). *The advance of the state in contemporary China.* Cambridge, UK: Cambridge University Press.

Elsa, Kania, Sacks, Samm, Triolo, Paul, & Webster, Graham. (2017). China's strategic thinking on building power in cyberspace. *New America.* URL: https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/ [September 25, 2017].

Feigenbaum, Evan. (2017). The deep roots and long branches of Chinese technonationalism. *Marco Polo.* URL: https://macropolo.org/deep-roots-long-branches-chinese-technonationalism/ [August 12, 2017].

Gan, Nectar. (2019). The complex reality of China's Social Credit System: Hi-tech dystopian plot or low-key incentive scheme? *South China Morning Post.* URL: https://www.scmp.com/news/china/politics/article/2185303/hi-tech-dystopia-or-low-key-incentive-scheme-complex-reality?utm_medium=Social&utm_source=Facebook&fbclid=IwAR2pMOeDkSbgTHwky4CLI1yMbB58n_jsEiTU666Xz2chHxSTjA7Dy4iRmv4 [Feburary 19, 2019].

Global Times. (2018). Many netizens take issue with Baidu CEO's comments on data privacy. *Global Times*. URL: http://www.globaltimes.cn/content/1095288.shtml [March 26, 2018].

Greenleaf, Graham, & Scott Livingston. (2017). China's Personal Information Standard: The Long March to a Privacy Law. *150 Privacy Laws & Business International Report*, 25–29.

Harwit, Eric. (2008). *China's telecommunication revolution*. Oxford, UK: Oxford University Press.

Hawkins, Amy. (2018). Beijing's big brother tech needs African faces. *Foriegn Policy*. URL: https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/ [July 24, 2018].

Hong, Yu. (2017a). Pivot to internet plus: Molding China's digital economy for economic restructuring? *International Journal of Communication*, *11*, 1486–1509.

Hong, Yu. (2017b). *Networking China: The digital transformation of the Chinese economy*. Champaign, IL: University of Illinois Press.

Hong, Yu. (2017c). Reading the 13th five-year plan: Reflections on China's ICT Policy. *International Journal of Communication*, *11*, 1755–1774.

Hornby, Lucy, Ju, Sherry, & Lucas, Louise. (2018) China cracks down on tech credit scoring. *Reuters*. URL: https://www.ft.com/content/f23e0cb2-07ec-11e8-9650-9c0ad2d7c5b5 [Feburary 4, 2018].

ISC. (2017). The personal information protection committee of ISC set up in Beijing. *Internet Society of China*. URL: http://www.isc.org.cn/english/Events&News/ISC_Events/listinfo-35986.html [January 24, 2017].

Jia, Lianrui. (2018). Going public and going global: Chinese internet companies and global finance networks. *Westminster Papers in Communication and Culture*, *13*(1), 17–36.

Jiang, Min, & Fu, King-Wa. (2018). Chinese social media and big data: Big data, big brother, big profit? *Policy and Internet, 10*(4), 372–392. doi: 10.1002/poi3.187

Keane, Michael, & Wu, Huan. (2018). Lofty ambitions, new territories, and turf battles: China's platforms "Go Out." *Media Industries,* 5(1), 51–68. doi: 10.3998/mij.15031809.0005.104

Knockel, Jeffery, Ruan, Lotus, Crete-Nishihata, Masashi, & Deibert, Ronald. (2018). (Can't) picture this: An analysis of image filtering on WeChat moments. *The Citizen Lab*. URL: https://citizenlab.ca/2018/08/cant-picture-this-an-analysis-of-image-filtering-on-wechat-moments/ [August 14, 2018].

Kobie, Nichole. (2019). The complicated truth about China's Social Credit System. *Wired*. URL: https://www.wired.co.uk/article/china-social-credit-system-explained [Janurary 21, 2019].

Kostka, Genia. (2019). China's Social Credit Systems and public opinion: Explaining high levels of approval. *New Media & Society*, *21*(7), 1565–1593. doi: https://doi.org/10.1177/1461444819826402

Kuo, Lily. (2019, March 1). China bans 23m from buying travel tickets as part of "Social Credit" System. *Guardian*. URL: https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system [March 1, 2019].

Lee, Jyh-An. (2018). Hacking into China's cybersecurity law. *Wake Forest Law Review*, *53*, 57–104.

Liang, Fan, Das, Vishnupriya, Kostyuk, Nadiya, & Hussian, Muzammil. (2018). Constructing a data-driven society: China's Social Credit System as a state surveillance infrastructure. *Policy & Internet*, *10*(4), 415–453. doi: 10.1002/poi3.183

Liang, Guo. (2006). Under the "Golden Shine": China's efforts to bridge government and citizens. Chinese academcy of social sciences, centre for social development. *Chinese Academcy of Social Sciences*. [January 28, 2006]

Lin, Liza, & Chin, Josh. (2017). China's tech giants have a second job: Helping Beijing spy on its people. *The Wall Street Journal*. URL: https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284 [November 30, 2017].

Maasho, Aaron. (2013). Ethiopia signs $800 million mobile network deal with China's ZTE. *Reuters*. URL: https://www.reuters.com/article/us-ethiopia-china-telecom/ethiopia-signs-800-million-mobile-network-deal-with-chinas-zte-idUSBRE97H0AZ20130818 [August 18, 2013].

Mandhana, Niharika. (2019). Huawei's video surveillance business hits snag in Philippines. *The Wall Street Journal*. URL: https://www.wsj.com/articles/huaweis-video-surveillance-business-hits-snag-in-philippines-11550683135?mod=e2twa [Feburary 20, 2019].

Meissner, Mirjam. (2017). China's Social Credit System: A big-data enabled approach to market regulation with broad implications for doing business in China. *Mercator Institute for China Studies*. URL: https://www.merics.org/sites/default/files/2017-09/China%20Monitor_39_SOCS_EN.pdf [May 24, 2017].

Mistreanu, Simina. (2018). Life Inside China's Social Credit laboratory: The party's massive experiment in ranking and monitoring Chinese citizens has already started. *Foreign Policy*. URL: https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/. [April 3, 2018]

Ranking Digital Rights. (2017). 2017 Corporate accountability index. *New America Foundation*. URL: https://rankingdigitalrights.org/wp-content/uploads/2017/04/RDRindex2017report.pdf [March 15, 2018].

Reuters. (2018a). China to bar people with bad "Social Credit" from planes, trains. *Reuters*. URL: https://www.reuters.com/article/us-china-credit/china-to-bar-people-with-bad-social-credit-from-planes-trains-idUSKCN1GS10S [March 16, 2018].

Reuters. (2018b). China's cyber watchdog scolds Ant financial over user privacy breach. *Reuters*. URL: https://www.reuters.com/article/us-ant-financial-china/chinas-cyber-watchdog-scolds-ant-financial-over-user-privacy-breach-idUSKBN1F006B [Janurary 10, 2018].

Sacks, Samm. (2018). China's emerging data privacy system and GDPR. *Center for Strategic & International Studies*. URL: https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr [March 9, 2018].

Sacks, Samm, Shi, Mingli, & Webster, Graham. (2019). The evolution of China's data governance regime: A timeline. *New America*. URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/china-data-governance-regime-timeline/ [Feburary 8, 2019].

Shanghai Securities News. (2017). Geren Zhengxin Paizhao Weihe Chidao Shangwu Jigou Da Jianguan Biaozhun. *CNstock*. URL: http://news.cnstock.com/news,yw-201704-4067613.htm [April 24, 2017].

Shen, Hong. (2016). China and global internet governance: Toward an alteranative analytical framework. *Chinese Journal of Communication, 9*(3), 304–324. doi: https://doi.org/10.1080/17544750.2016.1206028

Soo, Zen. (2018). Alibaba's payments affiliate apologises for opting in users for credit scoring system. *South China Morning Post*. URL: https://www.scmp.com/tech/china-tech/article/2126772/chinas-ant-financial-apologises-over-alipay-user-data-gaffe [20 July 20, 2018].

Southern Metropolis. (2017). Wangzhan he App Baohu Nide Yinsi le ma? *Southern Metropolis Daily*. URL: https://m.mp.oeeee.com/a/BAAFRD000020170531390 95.html [May 31, 2017].

Southern Metropolis. (2018). Wanganfa Sibaitian, 18% App Rengwu Yinsi Zhengce. *Yinsi Huweidui*. URL: https://m.mp.oeeee.com/a/BAAFRD000020180723921 57.html [July 23, 2018].

State Council. (2014). Guowuyuan Guanyu Yinfa Shehui Xinyong Tixi Jianshe Guihua Gangyao (2014–2020) de Tongzhi. *Gov.cn*. URL: http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm [March 16, 2018].

State Council. (2015). Renmin Yinhang Yinfa Guanyu Zuohao Geren Zhengxin Yewu Zhunbei Gongzuo de Tongzhi. *State Council, The People's Republic of China*. URL: http://www.gov.cn/xinwen/2015-01/05/content_2800381.htm [Janurary 5, 2015].

Tencent. (2017). Ma Huateng: Tengxun Jiang Jixu Tigong Jichu Lingpeijian Ji Lianjie Nengli. *Tencent Technology*. URL: http://tech.qq.com/a/20170420/034261.htm [April 20, 2017].

Toffler, Alvin. (1980). *The Third Wave*. New York: Morrow.

van Dijck, Jose. (2014). Datafication, dataism, and dataveillance: Big data between scientific paradigm and ideology. *Surviellance & Society, 12*(2), 197–208. doi: 10.24908/ss.v12i2.4776

Wang, Min, & Jiang, Zuosu. (2017). The defining approaches and practical paradox of sensitive data: An investigation of data protection laws in 92 countries and regions and 200 data breaches in the world. *International Journal of Communication*, *11*, 3286–3305.

Wangluo Chuanbo Zazhi. (2017). Shuju Chujing Anquan Pinggu: Baohu Jichuxing Zhanlue Ziyuan de Zhongyao Yihuan. *Cyberspace Administration of China*. URL: http://www.cac.gov.cn/2017-08/07/m_1121443948.htm [August 7, 2017].

Webster, Graham, & Kim, Scarlet. (2018). The data arms race is no excuse for abandoning privacy. *Foreign Policy*. URL: https://foreignpolicy.com/2018/08/14/the-data-arms-race-is-no-excuse-for-abandoning-privacy/ [August 14, 2018].

Wu, Yanfang, Lau, Tuenyu, Atkin, David, & Lin, Carolyn. (2011). A comparative study of online privacy regulations in the U.S and China. *Telecommunications Policy, 35*(7), 603–616. doi: 10.1016/j.telpol.2011.05.002

Xinhua. (2015). China unveils internet plus action plan to fuel growth. *State Council*. URL: http://english.gov.cn/policies/latest_releases/2015/07/04/content_281475140165588.htm [July 4, 2015].

Xinhua News Agency. (2017). *Kejibu Zhaokai Xinyidai Rengongzhineng Fazhan Guihua Ji Zhongda Keji Xiangmu Qidonghui*. Cyberspace Administration of China. URL: http://www.cac.gov.cn/2017-11/16/c_1121964697.htm [November 6, 2017].

Xu, Duoqi, Tang, Shiya, & Guttman, Dan. (2019). China's campaign-style internet finance governance: Causes, effects, and lessons learned for new information-based approaches to governance. *Computer Law & Security Review*, 35(1), 3–14. doi: 10.1016/j.clsr.2018.11.002

Yuan, Elaine, Feng, Miao, & Danowski, James. (2013). "Privacy" in semantic networks on Chinese social media: The case of Sina Weibo. *Journal of Communication*, *63*(6), 1011–1031. doi: 10.1111/jcom.12058

Zhao, Yuezhi. (2000). Caught in the web: The public interest and battle for control of China's information superhighway. *Info, 2*(1), 41–66. doi: 10.1108/14636690010801311