

Article

The Market Value of Who We Are: The Flow of Personal Data and Its Regulation in China

Dong Han

School of Journalism, Southern Illinois University, Carbondale, IL 62901, USA; E-Mail: donghan@siu.edu

Submitted: 30 January 2017 | Accepted: 15 March 2017 | Published: 12 April 2017

Abstract

This article focuses on market-driven collection of personal data and its regulation in China. It argues that there is a growing demand for personal data from China's advertising, marketing, and credit reporting businesses. Meanwhile, the rapid development of the Internet, notably social media and e-commerce, has generated very large pools of personal data on digital platforms. These two factors contribute to the fast growth of both legitimate and illegitimate collection and exploitation of personal information. Chinese laws and regulations lag behind the market and are not ready to regulate personal data as a key economic resource. They scatter in a wide array of economic and social sectors and lack a coherent structure and effective enforcement mechanism. Unspecified overarching rationale, ambivalent market regulation, inadequate enforcement, as well as safety risks of governmental databases are problems that hinder the protection of personal data in China. The role and implications of the new Internet Security Law, entering into force in June 2017, remain to be seen.

Keywords

China; credit analysis; e-commerce; Internet; media law; personal data; privacy; social media

Issue

This article is part of a multidisciplinary issue of *Media and Communication*, edited by Epp Lauk (University of Jyväskylä, Finland) and Raul Reis (Emerson College, USA).

© 2017 by the author; licensee Cogitatio (Lisbon, Portugal). This article is licensed under a Creative Commons Attribution 4.0 International License (CC BY).

1. Introduction

The protection of personal data is a serious problem in China, especially on the Internet. About 70 percent of Chinese Internet users have had their personal information leaked, including names, phone numbers, home addresses, ID card numbers, and workplace information (Ni, 2004; Z. Yang, 2016). Students preparing for exams receive phone calls and text messages that try to sell them preparation materials and books (Han Li, 2014). Credit card holders' information were sold online for prices as low as 2,000 *yuan* (US\$290) for one hundred thousand records (Lin Wang, 2015). In a national survey that collected more than one million responses, 81 percent surveyed have received phone calls from unfamiliar numbers appearing to know their personal information (Sohu.com, 2016). Illegal collection and sale of personal data have become an underground industry (Dong, 2012; J. Wang et al., 2016). In the first quarter of 2015, more

than one billion personal data records were illegally disclosed (Lin Wang, 2015). In 2016, an investigative news story found that 700 *yuan* (US\$100) can buy information on the whereabouts of just any person, including the exact time that she/he checked into a hotel room (J. Wang et al., 2016).

This article examines the growing market of personal data in China and its regulation by law. The protection of personal data is generally considered a privacy issue. In Nissenbaum's (2010) theoretical framework of contextual integrity, privacy is about the flow of personal information, defined as "information about an identifiable person" (p. 4). To address the problem of data privacy is not "simply *restricting* the flow of information but ensuring that it flows *appropriately*" (Nissenbaum, 2010, p. 2, emphasis original), and the regulation of personal data is in essence to adjudicate on the legitimacy of "novel flows of information" (p. 232) in specific contexts. Drawing on her arguments, matters of personal data in present-day

China need to be examined first and foremost as growing and transforming flows of individual-related information. The key questions are how to contextualize the growth of such flows, how to conceptualize the generation, collection, usage, transfer, and disposal of personal data, and how current law and regulations intervene and address privacy-related controversies.

Situating data flows in market and economic contexts, this article argues that personal data in China are commodified information produced and circulated to serve the need of businesses including advertising, marketing, personal lending, and credit reporting. Data acquisition, processing, and transfer are market activities centering on the control and trading of personal information as an important economic resource. Therefore, the regulation of personal data is essentially market regulation that governs a key profit-generating resource, and must be assessed and evaluated as such. China's laws and regulations lag behind the market, lack a coherent structure, and are not properly enforced. By recognizing the key role of the market in fostering personal data flow in present-day China, this research provides a contextualized analysis of legal development and highlights an often-neglected economic aspect of Chinese laws and regulations.

The following first examines the market and industry of personal data and documents the explosive growth of data flows as part of China's economic and Internet development. The next section overviews the transformation of the law and identifies key components in the regulatory framework. The Discussion section addresses a number of problems in China's personal data laws and regulations, including unspecified overarching rationale, ambivalent market regulation, inadequate enforcement, as well as safety risks of governmental databases. The Conclusion recaps the main points and briefly considers topics for future research.

2. The Market and Industry of Personal Data

While market-oriented personal data collection is not new to China, the rapid development of the Internet has brought about profound changes. On the one hand, the explosive growth of advertising, marketing, personal lending, and credit reporting businesses, often integrated with digital technologies and the Internet, has generated tremendous demand for personal data. On the other hand, social media, e-commerce sites, and other new media applications have put together large pools of individual information. The gathering, processing, and trading of personal data have become a huge market as well as a hotbed for unethical and illegal activities.

2.1. Growing Market Demand for Personal Data

China's advertising industry has had impressive growth since the turn of the century, and Internet-based adver-

tising and marketing have been at the forefront of the growth. Slowing down from 35 percent annual growth in the early 2000s (Lee, 2012), China's advertising industry is expected to maintain two-digit growth through the late 2010s with Internet advertising as the fastest growing sub-sector (Efnchina.com, 2014). From 2002 to 2005, Internet advertising revenue increased at an annual rate of 79 percent, significantly exceeding those in television and newspapers sectors at 15 percent and 11 percent, respectively (Meyer, Michael, & Nettesheim, 2009). Between 2006 and 2015, Internet advertising maintained two-digit annual growth (China Industry & Commerce News, 2015; H. Yang, 2013; X. Yang, 2014; Zhang, 2011), sometimes as high as 75.4 percent (Zhang, 2011). In 2014, Internet advertising total reached 157 billion *yuan* (US\$23 billion) (China Industry & Commerce News, 2015), nearly eight times that of 2009's 20.7 billion *yuan* (US\$3.1 billion) (Zhang, 2011). It is expected to reach 400 billion *yuan* (US\$58 billion) in 2018 and to take up 40 percent of the advertising industrial total (Efnchina.com, 2014). Shifting away from mass marketing toward more precise, targeted models in the digital environment (Hongmei Li, 2016), advertising in China has resulted in ever-increasing market demand for information on potential customers not as faceless consumers but as individuals with different preferences and needs.

The fast-growing personal loan industry is also hungry for information on customers. China's housing reform over the past two decades, which moved away from state-provided housing and encouraged home ownership, has created a huge market for housing as well as personal mortgage. The rapidly expanding home loan market has pushed traditional loan operations, based on the experience and judgment of mortgage personnel, to its limits and calls for a standard credit risk management tool to efficiently measure every potential borrower's creditworthiness (Gan, Li, Wang, & Kao, 2012). Meanwhile, as part of the Chinese state's policy to encourage consumer spending to boost economic growth, consumer loans have been quickly on the rise (Gough, 2016; Y. Wang, 2016). In 2016, there are 630 banks, about 2,500 peer-to-peer lending platforms, 9,000 small loan companies as well as a number of large consumer financial services and Internet-based businesses competing in the personal loan industry (Hu, 2016). Online lending "boomed" in the early 2010s and outstanding loans of peer-to-peer lending increased fourteen times from the start of 2014 to the end of 2015, reaching 440 billion *yuan* (US\$66.8 billion) (Fung & Magnier, 2016). In 2015, the consumer financing market exceeded nine trillion *yuan* (US\$1.3 trillion), and consumer loan total is expected to reach 37 trillion *yuan* (US\$5.4 trillion) in 2019 (Hu, 2016). Meanwhile, however, credit risk management has been a serious problem, and bad loans take up 13 to 17 percent of online lending (Hu, 2016). China's credit reporting system, as discussed below, cannot meet the demand of the loan industry. Lenders eager to issue loans to people with little or none financial his-

tory, which is not uncommon in China, have been found to use all sorts of means to guarantee returns, including asking for women's nude selfies as loan collaterals (Y. Wang, 2016). The industry is in dire need for something that can help to understand their potential customers' financial profiles better.

2.2. Data Pools of Personal Information on the Internet

The growth of social media, e-commerce, and Internet-based financial activities in China has created a very large stock of personal data. While the number of microblog users has stabilized in the past few years with a slight decrease from 274 million (June 2012) to 242 million (June 2016) (China Internet Network Information Center [CNNIC], 2012b, 2016), China's messaging applications, like WeChat and QQ, have accumulated huge numbers of users (760 million and 860 million, respectively) (Heine, 2016). Although Chinese Internet users tend to be on guard against explicit data collecting activities (Z. Wang & Yu, 2015), they are more likely (compared with their US counterparts) to share their experience and information on social media platforms, even with strangers (Nemati, Wall, & Chow, 2014). A CNNIC social media report in 2012 shows that 62 percent users trust social media sites' protection of their personal data, and over 70 percent do not mind their information being used for commercial purposes, as long as it is not leaked (CNNIC, 2012a, pp. 28–29). Given widespread leakage of personal data on the Chinese Internet, such trust is less about how well personal data are protected but more about Chinese users' insensitivity toward risks associated with social media postings (CNNIC, 2012a). As a matter of fact, China's social media sites provide such "a mountain of mobile data" that "advertising players are nearly salivating at the opportunities" (Heine, 2016).

In addition to social media, China's e-commerce sites also contribute significantly to the "mountain" of personal data. While industrial observers in 2009 still maintained that "[e]-commerce in China is years behind the West" (Meyer et al., 2009, p. 25), the early 2010s saw a massive growth. Online shopping in China kept an annual growth rate of 71 percent from 2009 to 2012 (S. Wang & Pfanner, 2013). In 2012, Chinese consumers ordered US\$210 billion worth of goods online and Alibaba alone processed US\$170 billion, more than the US's eBay and Amazon combined (China Economic Review, 2013). Mobile commerce (or m-commerce), retail through mobile devices like smart phones, almost tripled between 2011 and 2012 (China Economic Review, 2013). By June 2016, China had 448 million online shoppers, out of which 401 million shopped through their mobile phones, and 455 million people had used some form of online payment (CNNIC, 2016). On November 11, 2016, the so-called Single's Day (a newly invented one-day sales event), Alibaba posted nearly US\$18 billion in sales in 24 hours (The Economist, 2016a). Huge numbers of individuals shopping for goods and services online create

a very large data pool that contains information on their names, addresses, bank accounts, credit cards, financial profiles, shopping preferences, and sometime personal life situations.

2.3. Market-Driven Exploitation of Personal Data

Market-driven exploitation of personal data in China started decades earlier than the Internet, yet digital technology has brought about profound changes to the collection, processing, and transfer of personal and private information. This sub-section first overviews a more "traditional" form of personal data collection, and then examines new dynamics in the digital environment.

Credit reporting, which involves collection of individual's banking and credit records to assess one's creditworthiness, has had a long history in contemporary China and with significant involvement of leading transnational companies. Dunn & Bradstreet Corp had been on the Chinese market since the 1980s (People's Bank of China, 2013). In 1999, China's first personal credit reporting company started business in Shanghai (People's Bank of China, 2013). In January 2006, the People's Bank of China's (China's central bank) personal credit information database started operation (People's Bank of China, 2013). By the end of 2015, the database had grown to cover 880 million people, 380 million of which had credit histories (Hu, 2016). Over the past decade, the central bank's personal credit information database has played an important role to assist banks to assess individual customer's creditworthiness in loan decisions.

However, the inadequacies of the central bank's database are dramatically amplified when market need for personal data rocketed and when Internet growth generated huge amounts of consumer information. As a matter of fact, the database has never been sufficiently large. It relies on banking and credit information from banks across the country, but only 79 percent of Chinese people above the age of 15 have bank accounts, and only 10 percent have borrowed from banks (Gough, 2016). It is estimated that the database only effectively covers 35 percent of the population (Hu, 2016), and can only fulfill a quarter of market need for personal credit reporting (Weiland, 2015). In addition, consumer information on e-commerce platforms and social media sites, priceless resources for market players, are not part of the bank's database. It thus cannot fully meet the demand of the market in the fast-growing economy.

Filling in the gap are numerous large and small businesses fervently working to create individual consumer profiles out of personal data available on the Internet. In "probably the largest untapped consumer finance market globally" (Gough, 2016), credit reporting in China is potentially a 100 billion *yuan* (US\$14.5 billion) business (Weiland, 2015). Chinese Internet giants have all created credit rating subsidiaries to make full use of their user bases. For example, Alibaba's Ant Financial Services gathers data from more than 300 million real-name regis-

tered users, transaction records on Taobao and Tmall, payment histories on Alipay (similar to Paypal) and investment activities on Yu'e Bao (an online money market fund with 150 million users), all of which part of Alibaba's gigantic corporate complex (Gough, 2015). Meanwhile, Tencent's credit rating subsidiary, Tencent Credit Bureau, uses massive data on social media like QQ as well as from Tencent's Internet security applications (Chen, 2015) and has discovered that social media data can significantly help with credit risk analysis (Lin, 2015).

In this nascent and fast-growing industry, new credit rating businesses use all kinds of "non-traditional" methods to collect and process personal data, many of which borders on privacy infringement. In addition to off-line investigations that look into court records, restaurant files, transportation data, "number of toothbrushes or towels" in bathrooms, and "dirty dishes in the kitchen" (Gough, 2016; Y. Wang, 2016), credit rating companies track one's digital footprint to look for anything that may inform them of a potential borrower's likelihood of default. Information deemed useful include "social-network connections, web-browsing habits, how they fill out online forms and their online purchases" (Lohr, 2015), search histories and online chatting records (Gough, 2016; Y. Wang, 2016), as well as one's social circles and friends' creditworthiness (Clover, 2016). Some cell phone applications collect "hundreds of details" from a potential borrower (Gough, 2016) so as to "provide a 360 degree portrait of the borrowers' personal lives" (Y. Wang, 2016).

Advertisers and marketers, in addition to credit rating and reporting businesses, are after the opportunities of targeted marketing offered by vast volumes of personal data. On the one hand, social media have become the virtual "town square" for advertising and marketing, and China is catching up on using big data to manage customer relationship. Major brands including Burberry, Mercedes-Benz, Michael Kors, Yves Saint Laurent, Kate Spade, and Montblanc have all been utilizing data generated from messaging applications like WeChat (Heine, 2016). On the other hand, large amounts of personal information from dubious sources are sold to marketers and advertisers, sometimes at very low prices (Han Li, 2014). Chinese consumers are bombarded by marketing calls, messages, and emails, which appear to know exactly what they need at the moment (Han Li, 2014; Qiu, 2014). Illegal acquisition and transfer of personal data are not confined to underground organizations. In 2013, a Dunn & Bradstreet Corp's subsidiary in Shanghai was fined one million *yuan* (US\$145,000) and four executives were jailed for illegally purchasing large volumes of personal data and selling them to advertisers (Chu, 2013; Dong, 2012). In spite of repeated lawmaking and policing efforts, the trading of illegally obtained personal data persists, partly because the market demand for such data is very strong (Ni, 2014).

Apart from legitimate businesses, personal data also have other buyers. Documented public sale of personal

data can be traced back to 2006, when a website claimed to have personal information, including phone numbers, addresses, marital status, etc., on 90 million people and offered to sell to anyone with a cell phone (Zhu, 2006). In the 2010s and with astronomical amounts of personal data flowing on the Internet, personal information becomes the target of rampant criminal activities. In the words of a researcher, cases of fraud, blackmail, rape, and kidnapping that can be attributed to personal information leakage "are not even news" in present-day China (Han Li, 2014). In 2016 alone, Chinese police cracked more than 1,800 criminal cases involving illegal acquisition and trading of personal data (Xinhua News Agency, 2016). Among other crimes, personal data and information are used widely in various fraudulent activities. In 2016, a fraudulent phone call won the trust of an 18-year-old because it knew all the details of her application for financial aid for college. Having lost the family's years of savings for her college expenses, Xv Yuyu had a heart attack and died (X. Wang, 2016). Personal data in China call for effective regulation, to which the next section will turn.

3. The Development and Transformation of Laws and Regulations

China has a large number of laws and regulations that pertain to personal data protection. A researcher working at the Ministry of Industry and Information Technologies (MIIT) counts about 40 laws (enacted by the National People's Congress [NPC], the supreme legislature), 30 regulations (promulgated by the State Council, the cabinet-style central government), and 200 lower-level rules that protect personal information (Guo & Wu, 2012). These laws and regulations scatter in a number of industrial and social sectors without a coherent structure, creating problems for law enforcement, the industry, as well as individuals seeking protection.

A key issue is the growth of privacy law in China. In the Chinese context, privacy is "a sweeping term encompassing everything from the quest for personal dignity and safety to the growing sense of political participation" (Yuan, Feng, & Danowski, 2013, p. 1029). Privacy-related clauses in Chinese Constitutions and laws have a long history. As early as 1954, the first Constitution of the People's Republic of China explicitly protected individual's residence and mail's security in Article 90. Starting the 1980s, laws, regulations, and the Supreme People's Court's (SPC, the supreme judicial organ) opinions gradually built up China's privacy law. The Tort Liability Law of 2009 formally recognizes the right to privacy, and an SPC Judicial Interpretation in 2014 (Rules Concerning Several Issues in the Adjudication of Civil Cases of Infringement on Personal Rights through Information Networks) defines the scope of private information in the digital setting as well as exemptions of privacy infringement. As part of contemporary Chinese law that "has developed perhaps faster than any legal system in history" (Lieb-

man, 2011, p. 167), privacy law in China has had dramatic growth in a short amount of time.

However, a large part of privacy law has little to do with personal data. Significant attention in privacy law development is devoted to line-drawing between private information that a person rightfully expects to keep undisclosed, and other information that one does not mind sharing. For example, an individual's medical history is protected under privacy law, but the same rules may not work to keep her/his shopping preferences secret, since the two types of information are very different. An important case in Internet privacy, *Wang Fei v. Zhang Leyi* (2008), is about whether and how details of one's personal life can be published on the Internet. Yet its rules do not apply to a case in which telemarketers learn about one's need for baby clothes, since having a newborn in the family is not information unwilling to share. As Nissenbaum (2010) points out, "the private/public dichotomy" and "the attempt to define a category of sensitive information" (p. 232) are largely irrelevant in matters of data privacy. In relation to Chinese law, Liming Wang (2012) argues that there are four significant differences between privacy and personal data protection. Notably, privacy is about preventing disclosure of certain facts, but personal data protection is about the control and exploitation of information that may or may not be private. While they do share much in common, the protection of privacy "may fare far better" than personal data protection under Chinese law, since they rely on different mechanisms (de Hert & Papakonstantinou, 2015, p. 14). The law of personal data protection in China has distinctive features and structure of its own.

Among the two hundred plus laws, regulations, and rules on personal data protection before November 2016, five laws/regulations are noteworthy. In December 2012, the Standing Committee of the NPC passed the Decision on Strengthening Network Information Protection (2012 Decision). Enacted by the permanent body of the supreme legislature, 2012 Decision sets forth a preliminary framework for personal data protection on the Internet. It recognizes that there are two types of personal data: those that lead to identification of individuals and those pertinent to individual privacy. It stipulates that the collection of personal data must be "legal, legitimate, and necessary (*hefa, zhengdang, biyao*)", and that the methods of data collection and utilization must be open and published. It also requires Internet service providers and governmental employees to ensure that personal data under their control be kept secure.

In 2013, an amendment to the Consumer Rights Protection Law created protection for consumer data and information. It incorporates the NPC's 2012 Decision and spells out a number of principles of personal data protection (Gao & O'Sullivan-Gavin, 2015). Its Article 14 stipulates that the protection of consumers' personal information is on a par with the protection of "human dignity (*rengē zunyan*)". Article 29 stipulates that the collection of personal information must be "legal, legitimate,

and necessary" (principles from the 2012 Decision), must obtain prior consent, and must take security measures to prevent leakage. In addition, Article 56 treats the infringement of personal data security the same as a number of fraudulent and deceptive commercial activities, which are subject to administrative penalties including fines and forced shutdowns.

The MIIT's Information Security Technology—Guidelines for Personal Information Protection Within Information System for Public and Commercial Services (2013 Guidelines), effective in 2013, is another noteworthy rule-making effort. It aims to create a systematic framework of personal data protection in computer and information networks. 2013 Guidelines draws a line between "personal sensitive information" and "personal general information", the former referring to information that "would have an adverse impact on the subject of personal information if disclosed or altered" including one's ID card number (similar to social security number in the US), biometric information, etc. It sets forth eight "basic principles", including personal consent, public notification, and minimum sufficiency, that govern the whole process of personal data collection and processing. Overall, the 2013 Guidelines has a "very careful structure and considerable detail", suggesting that "China is moving away from having a patchwork of largely unrelated sectoral data privacy laws (somewhat like the US) toward a more coherent structure" (Greenleaf & Tian, 2013, p. 6). However, it is not backed by law enforcement but asks for voluntary industrial cooperation. Issued in November 2012 as a voluntary compliance guide with a GB/Z serial number, it was required by law to go through reevaluation in three years, which did not happen on its expiration date in 2015 and rendered its legal status uncertain.

The Administrative Regulations of the Credit Information Industry of 2013, promulgated by the State Council, is an important but often-neglected legal instrument that governs personal data collection. Its definition of "credit information activities (*zhengxin yewu*)" in Article 2 includes the collection, compiling, storing, processing, and reporting of individual credit information, and its Article 3 expressly prohibits infringement on privacy. It has a full chapter, Chapter 3, which contains comprehensive provisions on the handling of personal data as well as individual rights including access and rectification. Its authority covers the rapidly growing industry of credit analysis and reporting, in which private businesses rely heavily on data mining that often verge on privacy infringement. Given the ascending role of credit analysis businesses in the flow of personal data in China, the Administrative Regulations is not merely a sectoral legislation but has a significant role in data privacy regulation as a whole.

Another important personal data protection law is China's Criminal Law, which has two amendments over the past decade that address personal data security. In 2009, the Seventh Amendment to the Criminal Law crim-

inalized both “illegal sale and provision of personal information” and “illegal acquisition of personal information”. In 2015, the Ninth Amendment to the Criminal Law combined the two into “infringement on personal information” and raised the maximum penalty from three years to seven years in jail. In the early 2010s, news coverage of police crackdown on illegal acquisition and trading of personal data abounds (see Ni, 2014; X. Wang, 2016; Xinhua News Agency, 2016). However, convictions of personal data-related crimes tend to be inconsistent and too lenient to be effectively deterrent (Y. Li, 2016). Statistics suggest that personal data leakage has continued to grow. While the second half of 2013 witnessed 19.63 billion *yuan* (US\$2.8 billion) of economic loss caused by personal information leakage (Qiu, 2014), that figure more than doubled and jumped to 91.5 billion *yuan* (US\$13.3 billion) during the one-year span from mid-2015 to mid-2016 (Y. Li, 2016).

In November 2016, the NPC passed the Internet Security Law, which will enter into force in June 2017. The law has a full chapter, Chapter 4, devoted to personal data security. It inherits principles from the 2012 Decision and significantly elaborates on a number of fronts. While “the basics of international data protection are not unequivocally in place” in pre-2015 Chinese law (de Hert & Papakonstantinou, 2015, p. 6), the Internet Security Law “systematically defines personal data protection” and is “highly in line with (*gaodu jiegui*) international best practices and other countries’ laws and regulations on personal information protection” (Deloitte, n.d.). By comparing the law with the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, consultancy Deloitte (n.d.) argues that all nine principles of the APEC Framework, including “preventing harm”, “notice”, and “collection limitations”, are fully realized in Chinese law. As a newly minted statute not yet enforced, its role and implications in China’s digital data protection system remain to be seen.

4. Discussion

Personal data protection in China is a legal issue as well as a market issue. It is about individual’s life tranquility as well as a bulging industrial sector that increasingly see personal data and information as key economic resources. In the words of Ant Financial Services’ chief technology officer, users’ personal information, including family, career, online shopping and payment history, are “oil and gold of the future (*weilai de shiyou huangjin*)” (Xie, 2015). The regulation of personal data is, among other things, market regulation of a key economic resource and needs to be assessed accordingly.

To define and to protect personal data is to draw a line between acceptable commercial practices and individual control over information on her/his life. From the perspective of market forces seeking to utilize personal data, less control by individuals means fewer restrictions on their business practices. Thus, lawmaking is

not a context-free process but a balancing act between two conflicting interests. Between these two, market-oriented interests have ample support from the Chinese state, which has persistently pushed for economic growth in Internet-related sectors. Moreover, China has recently called for intensified integration of digital technology in the economy through the so-called “Internet Plus” strategy, unveiled in Premier Li Keqiang’s Governmental Work Report in 2015 and with emphases on big data, e-commerce, and Internet finance. In contrast, the ideological and policy basis for protecting individual control over her/his life details is not well-articulated. While the basis of EU’s personal data regime is human rights protection (de Hert & Papakonstantinou, 2015), China seems speechless on why individuals can control information on who they are and what they do. Major laws and regulations, including the Internet Security Law, 2012 Decision, and 2013 Guidelines, shun away from articulating their *raison d’être*. An interesting exception is the Consumer Rights Protection Law, which claims to protect consumers’ “human dignity” but does not elaborate. In the face of aggressive, market-oriented exploitation of personal data, it remains to be seen how the lack of a well-articulated ideological basis for data protection may impact future law and policy-making.

As a matter of fact, on-going commercial experiments on personal data in China are already beyond what would be tolerated under the laws of major Western countries. Social media companies in the West have long been eyeing the possibilities of mining user data for credit analysis. For example, Mark Zuckerberg, chairman and CEO of Facebook, holds a patent that “allows lenders to assess creditworthiness based on the credit ratings of people in a borrower’s network” (Demos & Seetharaman, 2016). It was regulatory concerns, notably a report by the Federal Trade Commission, that put a halt to the emerging business practice (Demos & Seetharaman, 2016). Meanwhile, however, business models that would “fail miserably” under US law are thriving in China (Kapron, 2016). One of the pioneer players in big data-based credit analysis, ZestFinance, has founded a joint-venture with a leading Chinese online retailer, JD.com, to offer credit-analysis service to lenders all over China (Lohr, 2015). It seems that the Chinese government recently became aware of the situation. Having asked eight private non-banking businesses to prepare for credit reporting operations in early 2015, the People’s Bank of China has not issued any license under the Administrative Regulations of the Credit Information Industry as expected. Instead, the central bank issued a regulatory guidance in late 2015 out of data privacy concerns (Mei & Liu, 2015). Among other things, the guidance requires a credit reporting business, once licensed, to make a security deposit of at least five million *yuan* (US\$725,000) for possible damages and liabilities to privacy-infringed individuals (Mei & Liu, 2015). Nevertheless, no specific market policies have been formulated to draw a line between what can and cannot be done, while private busi-

nesses including Alibaba and Tencent are moving fast on their experimentations.

Current Chinese law and enforcement do not seem ready to regulate the collection and trading of personal data as a key economic resource. For “oil and gold” of the future, the regulatory *status quo* seriously lacks strength and effectiveness. Scattered in a number of laws and regulations, personal data protection does not have a centralized enforcement mechanism (Greenleaf, 2014, pp. 191–226). It is only through a reading of a multitude of legal instruments that one can find a “cumulative effect” of data protection in the absence of an overarching framework (de Hert & Papakonstantinou, 2015, p. 22). The enforcement of existing laws and regulations, including the Criminal Law, does not offer sufficient protection or show much deterrent power, as the court tends to be very lenient with personal data-related crimes. In spite of rampant data security problems, the number of criminal convictions between 2010 and 2015 was very small (Lin Wang, 2015). While an amendment to the Criminal Law in 2015 increased maximum jail time from three years to seven years, the most severe conviction between 2015 and 2016 only handed down a two-year sentence with a two-year probation (Y. Li, 2016), which means the perpetrator will not be jailed unless she/he commits another crime during the probationary period. As a senior official at the Ministry of Public Security points out, the “costs” of such crimes are very low (Ni, 2014).

Another problem is the security of databases under the control of governmental agencies and public institutions. Chinese laws and regulations on personal data tend to target private enterprises, and seldom impose similar restrictions on the government (de Hert & Papakonstantinou, 2015). The legitimacy of governmental collection of personal data is often taken for granted (Wu, 2014). Moreover, the law often expressly requires Internet service providers to hand data over to the government in broadly defined scenarios. China’s governmental agencies and public institutions (e.g., universities and schools) have compiled tremendous volumes of personal information with minimum constraints from law or through self-regulation. While 72.5 percent of commercial websites in China have some kind of privacy disclosure notice (Stanaland & Lwin, 2013), Chinese governmental sites generally do not have privacy policies or notices (Shan, 2008). These databases are often vulnerable in the face of profit-driven activities. In spite of a number of laws, including the Criminal Law, that prohibit governmental and public employees from disclosing personal information under their control, many data-related crimes rely on “insiders (*neigui*)” working in schools, state-owned banks and telecommunication companies, and the police (X. Wang, 2016). Another key threat comes from hacking and various theft techniques widely employed in China’s Internet-based underground economy (Zhuge, Gu, Duan, & Roberts, 2015), since a large portion of personal data crimes start with hacking online databases (X. Wang, 2016; Xinhua News Agency, 2016).

5. Conclusion

In China, growing market demand for personal information and the availability of large data pools on digital platforms give rise to both legitimate and illegitimate data collection activities. The current legal framework, with some uncertainties from the new Internet Security Law, is inadequate for the regulation of personal data as a critical economic resource.

This research focuses on the law of personal data as market regulation. A future research project can explore more on the ideological and political aspects. In addition to surveillance issues (Clover, 2016; Fry, 2015; The Economist, 2016b), it will be interesting to see when and how China, moving towards a centralized and more coherent regulatory structure (Gao & O’Sullivan-Gavin, 2015; Greenleaf, 2014, pp. 191–226), may come up with an overarching rationale for personal data protection. As de Hert and Papakonstantinou (2015) point out, current laws tend to treat individuals as consumers and subject data protection to e-commerce growth. The new Internet Security Law, however, places personal data under a broadly defined notion of “security”, which covers infrastructure security, network sovereignty, and national security. It remains to be seen how this new approach may contribute to the shaping of an overarching framework. Another noteworthy topic is data privacy and China’s anti-corruption campaign. The Chinese government devoted significant attention to the drafting of the Personal Data Protection Law during the 2000s, but the bill never entered the legislative pipeline partly due to resistance from some members of the bureaucracy. Some argue that a comprehensive personal data legislation must incorporate a definition of privacy that treats private persons and public figures differently (Hou, 2016; Lv, 2010), which was sternly opposed by governmental officials unwilling to disclose their property and financial information (C. Li, 2010; Lv, 2010). The Internet Security Law, focusing on data security and leakage prevention, does not address the issue. Whether a stand-alone personal data law will be enacted in the future, how it will define personal data and privacy, and how China’s anti-corruption endeavors may impact legal development, will worth scholarly attention.

Conflict of Interests

The author declares no conflict of interests.

References

- Chen, J. (2015). Zhima Xinyong yazhu xiaofei, Tengxin Zhengxin jintie jigou: Hulianwang zhengxin gezhan suochang [Sesame Credit focusing on consumption records, Tencent Credit working with financial institutions: Different strategies of Internet credit rating]. *Sina.com*. Retrieved from <http://finance.sina.com.cn/roll/20150825/080823054761.shtml>

- China Economic Review. (2013). Mobilizing the masses. *China Economic Review*. Retrieved from <http://www.chinaeconomicreview.com/mobilizing-masses>
- China Industry & Commerce News. (2015). Yongbao hulianwang, shixian xinkuayue: 2015 woguo guanggaoye fazhan liangdian shuping [Embracing the Internet, making a new leap-forward: A comment on China' advertising industry growth in 2015]. *Gov.cn*. Retrieved from http://www.saic.gov.cn/ggs/dfdt/201512/t20151217_165050.html
- China Internet Network Information Center. (2012a). *Research report on Chinese Internet users' use of social media in 2012*. Retrieved from <http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/sqbg/201302/P020130219611651054576.pdf>
- China Internet Network Information Center. (2012b). *The 30th Chinese Internet development survey report*. Retrieved from <http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201207/P020120723477451202474.pdf>
- China Internet Network Information Center. (2016). *The 38th Chinese Internet development survey report*. Retrieved from <http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201608/P020160803367337470363.pdf>
- Chu, K. (2013). Dun & Bradstreet fined, four sentenced in China. *The Wall Street Journal*. Retrieved from <http://www.wsj.com/articles/SB10001424127887323482504578230781008932240>
- Clover, C. (2016). China: When big data meets big brother. *Financial Times*. Retrieved from <https://www.ft.com/content/b5b13a5e-b847-11e5-b151-8e15c9a029fb>
- de Hert, P., & Papakonstantinou, V. (2015). *The data protection regime in China: In-depth analysis*. Retrieved from [http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA\(2015\)536472_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf)
- Deloitte. (n.d.). Zhongguo Wangluo Anquan Fa xilie jiedu zhiyi [Understanding the Chinese Internet Security Law: Part one]. *Deloitte.com*. Retrieved from <https://www2.deloitte.com/cn/zh/pages/risk/articles/cybersecurity-personal-information-protection.html>
- Demos, T., & Seetharaman, D. (2016). Facebook isn't so good at judging your credit after all. *The Wall Street Journal*. Retrieved from <http://www.wsj.com/articles/lenders-drop-plans-to-judge-you-by-your-facebook-friends-1456309801>
- Dong, R. (2012). Geren xinxi baohu guojia biao zhun ji-jiang chutai [National standards for personal data protection will be issued soon]. *Xinhuanet*. Retrieved from http://news.xinhuanet.com/legal/2012-03/26/c_122881744.htm
- Efnchina.com. (2014). Guanggao hangye shendu baogao: Weilai wunian shichang guimo huo chao wanyi [An in-depth report on the advertising industry: The industrial total may exceed one trillion yuan in the next five years]. *Efnchina.com*. Retrieved from <http://finance.cenet.org.cn/show-1514-57310-1.html>
- Fry, J. D. (2015). Privacy, predictability and internet surveillance in the U.S. and China: Better the devil you know? *University of Pennsylvania Journal of International Law*, 37(2), 419–501.
- Fung, E., & Magnier, M. (2016). China online financing firms face more regulatory tightening; Executives cite rising credit risks, potential new government restrictions. *The Wall Street Journal*. Retrieved from <https://www.wsj.com/articles/china-online-financing-firms-face-more-regulatory-tightening-1458737168>
- Gan, C., Li, Z., Wang, W., & Kao, B. (2012). Credit scoring in mortgage lending: Evidence from China. *International Journal of Housing Markets and Analysis*, 5(4), 334–350.
- Gao, Z., & O'Sullivan-Gavin, S. (2015). The development of consumer privacy protection policy in China: A historical overview. *Journal of Historical Research in Marketing*, 7(2), 232–255.
- Gough, N. (2015, January 29). Alibaba data to help provide consumer credit ratings. *The New York Times*, p. B9.
- Gough, N. (2016, October 11). Creditworthy in China. *The New York Times*, p. B1.
- Greenleaf, G. (2014). *Asian data privacy laws: Trade and human rights perspective*. New York, NY: Oxford University Press.
- Greenleaf, G., & Tian, G. (2013). China expands data protection through 2013 Guidelines: A "Third Line" for personal information protection. *Privacy Laws & Business International Report*, 122(1), 4–6.
- Guo, S., & Wu, P. (2012). Woguo jiang chutai geren xinxi baohu guojia biao zhun [China will produce national standards for personal information protection]. *China.com*. Retrieved from http://www.china.com.cn/policy/txt/2012-04/05/content_25063859.htm
- Heine, C. (2016, July 1). 8 data points that marketers need to know about China's biggest mobile player. *Adweek*, p. 13.
- Hou, Y. (2016). Huyu jinkuai chutai geren xinxi baohufa [A call to speed up the making of personal data protection law]. *Gov.cn*. Retrieved from http://www.npc.gov.cn/npc/zgrdzz/2016-11/16/content_2002121.htm
- Hu, Q. (2016). 8 jigou dengdai 19 ge yue; geren zhengxin paizhao weihe yizheng nanqiu [Eight companies waiting for nineteen months: Why still no license issued for personal credit reporting]? *Eeo.com.cn*. Retrieved from <http://www.eeo.com.cn/2016/0731/290366.shtml>
- Kapron, Z. (2016). Measuring credit: How Baidu, Alibaba and Tencent may succeed where Facebook failed. *Forbes*. Retrieved from <http://www.forbes.com/sites/zennonkapron/2016/03/17/measuring-credit-how-baidu-alibaba-and-tencent-may-succeed-where-facebook-failed>
- Lee, K. (2012). Zhongguo guanggao hangye fazhan xianzhuang yu qushi [Development and trend of

- China's advertising industry]. *People.cn*. Retrieved from <http://media.people.com.cn/n/2012/1029/c350882-19423103.html>
- Li, C. (2010). Guanyuan weihe dui caichan shenbao zhidu wufa dacheng shehui gongshi [Why governmental officials cannot reach a consensus on property disclosure]? *China Elections and Governance*. Retrieved from <http://www.chinaelections.org/article/62/191696.html>
- Li, H. [Han]. (2014). 130 wan kaoyanzhe xinxi bei jiaomai [1.3 million graduate school entrance exam takers' personal information for sale]. *Sina.com*. Retrieved from <http://news.sina.com.cn/c/2014-12-10/032331266499.shtml>
- Li, H. [Hongmei]. (2016). *Advertising and consumer culture in China*. Malden, MA: Polity.
- Li, Y. (2016). Qinfan gongmin geren xinxi de shijian yu xikao [Legal practices and analysis of criminal infringement on personal information]. *China Legal Science*. Retrieved from <http://www.iolaw.org.cn/showNews.aspx?id=55467>
- Liebman, B. L. (2011). A return to populist legality? Historical legacies and legal reform. In S. Heilmann & E. J. Perry (Eds.), *Mao's invisible hand: The political foundations of adaptive governance in China* (pp. 165–200). Cambridge and London: Harvard University Asia Center.
- Lin, J. (2015). Tengxin Zhengxin: Shejiao shuju yeneng pinggu xinyong [Tencent Credit Bureau: Social media data can be used to evaluate credit]. *Caixin*. Retrieved from <http://finance.caixin.com/2015-07-21/100830962.html>
- Lohr, S. (2015, June 29). ZestFinance takes big data credit scoring to China. *The New York Times*, p. B4.
- Lv, P. (2010). Dui guanyuan caican shenbao zhidu jizhong wudu de jixi [Analyzing several misunderstandings on disclosing governmental officials' property and financial information]. *People.cn*. Retrieved from <http://politics.people.com.cn/GB/30178/12330693.html>
- Mei, W., & Liu, X. (2015). Yanghang xiafa zhengxin jigou jianguan zhiyin [The central bank issues regulatory guidelines for information reporting institutions]. *Sina.com*. Retrieved from http://finance.sina.com.cn/money/bank/bank_hydt/20151202/014423904201.shtml
- Meyer, M., Michael, D. C., & Nettesheim, C. (2009). Reaching China's digital consumers: Advertising and marketing in China must join the online revolution. *China Business Review*, 36(1), 24–27.
- Nemati, H., Wall, J. D., & Chow, A. (2014). Privacy coping and information-sharing behaviors in social media: A comparison of Chinese and U.S. users. *Journal of Global Information Technology Management*, 17(4), 228–249.
- Ni, X. (2014). Geren xinxi xielu heshiliao [When will personal information leakage come to an end]? *People.cn*. Retrieved from <http://politics.people.com.cn/n/2014/0218/c369090-24389914.html>
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.
- People's Bank of China. (2013). *Zhongguo zhengxinye fazhan baogao 2003–2013 [Report on the development of credit information industry in China: 2003–2013]*. Retrieved from <http://www.gov.cn/gzdt/att/att/site1/20131212/1c6f6506c5d514139c2f01.pdf>
- Qiu, F. (2014). Renda daibiao jianyi zhiding geren xinxi baohufa [People's Congress representatives proposing enacting personal information protection law]. *Sina.com*. Retrieved from <http://news.sina.com.cn/c/2014-03-12/022129683720.shtml>
- Shan, F. (2008). Woguo geren xinxi baohu zhi xianzhuang [Current status of personal data protection in China]. *Chinacourt.org*. Retrieved from <http://www.chinacourt.org/article/detail/2008/03/id/291587.shtml>
- Sohu.com. (2016). Zhongguo geren xinxi anquan he yinsi baohu baogao [Report on personal data security and privacy protection in China]. *Sohu.com*. Retrieved from <http://mt.sohu.com/20161125/n474164242.shtml>
- Stanaland, A. J. S., & Lwin, M. O. (2013). Online privacy practices: Advances in China. *Journal of International Business Research*, 12(2), 33–46.
- The Economist. (2016a). Just spend: China's consumer credit-rating culture is evolving fast—And unconventionally. *The Economist*. Retrieved from <http://www.economist.com/news/finance-and-economics/21710292-chinas-consumer-credit-rating-culture-evolving-fastand-unconventionally-just>
- The Economist. (2016b). China invents the digital totalitarian state. *The Economist*. Retrieved from <http://www.economist.com/news/briefing/21711902-worrying-implications-its-social-credit-project-china-invents-digital-totalitarian>
- Wang Fei v. Zhang Leyi. Beijing Chaoyang District People's Court. Chao Min Chu Zi No. 10930. (2008).
- Wang, J., Rao, L., Li, L., Xiang, Z., Yang, A., & Wang, Q. (2016). 700 yuan nengmai duoxiang xingzong [700 yuan can buy a lot about your whereabouts]. *Sina.com*. Retrieved from <http://news.sina.com.cn/c/nd/2016-12-17/doc-ifxytqax6392517.shtml>
- Wang, L. [Liming]. (2012). Yisiquan gainian de zai jieding [Re-defining the right to privacy]. *Faxuejia*, 1, 108–120.
- Wang, L. [Lin]. (2015). Zhajin geren xinxi baohu de fazhi liba [Protecting personal data by law]. *Xinhuanet*. Retrieved from http://news.xinhuanet.com/finance/2015-08/06/c_128097826.htm
- Wang, S., & Pfanner, E. (2013, November 12). Chinese spree sets the record in online sales. *New York Times*, p. A1.
- Wang, X. (2016). Shui chumai le gongmin geren xinxi [Who sold people's personal information]? *The Paper*. Retrieved from <http://www.thepaper.cn/baidu.jsp?contid=1519523>

- Wang, Y. (2016). China wants to rate people's credit with online data, but misuse by companies is rampant. *Forbes*. Retrieved from <http://www.forbes.com/sites/ywang/2016/07/12/china-wants-to-rate-peoples-credit-with-online-data-but-misuse-by-companies-is-rampant/#5d8f444e116f>
- Wang, Z., & Yu, Q. (2015). Privacy trust crisis of personal data in China in the era of Big Data: The survey and countermeasures. *Computer Law & Security Review*, 31(6), 782–792.
- Weiland, D. (2015). Confusion abounds over China's emerging credit reporting industry. *South China Morning Post*. Retrieved from <http://www.scmp.com/business/banking-finance/article/1691579/confusion-abounds-over-chinas-emerging-credit-reporting>
- Wu, Y. (2014). Protecting personal data in e-government: A cross-country study. *Government Information Quarterly*, 31(1), 150–159.
- Xie, W. (2015). Qianyi geren zhengxin shichang zhong kaizha [Worth trillions: Individual credit information industry is open]. *Renmin Wenzhai*. Retrieved from http://paper.people.com.cn/rmwz/html/2015-04/01/content_1611170.htm
- Xinhua News Agency. (2016). Gonganbu fabu qinfan gongmin geren xinxi fazui shida dianxing anli [The Ministry of Public Security publishes ten criminal cases that infringe on personal information]. *Xinhuanet*. Retrieved from http://news.xinhuanet.com/legal/2016-12/17/c_1120136689.htm
- Yang, H. (2013). Jianchi yu shouwang: 2012 nian Zhongguo guanggaoye fazhan huigu yu qianzhan [Persistence and expectations: Looking back and forward at Chinese advertising industry in 2012]. *People.cn*. Retrieved from <http://media.people.com.cn/n/2013/0315/c359080-20804925.html>
- Yang, X. (2014). 2013 Nian zhongguo wangluo guanggao shichang guimo tupo qianyi daguan [Chinese Internet advertising industry in 2013 exceeded one hundred billion yuan]. *iResearch*. Retrieved from <http://a.iresearch.cn/others/20140109/224661.shtml>
- Yang, Z. (2016). Geren xinxi xielu wenti yanzhong; woguo jiang chutai shuju caiji guojia biao zhun [Personal data leakage is a serious problem; China will produce national standards for data collection]. *China Economic Net*. Retrieved from http://www.ce.cn/xwzx/gnsz/gdxw/201605/11/t20160511_11446795.shtml
- Yuan, E. J., Feng, M., & Danowski, J. A. (2013). "Privacy" in semantic networks on Chinese social media: The case of Sina Weibo. *Journal of Communication*, 63(6), 1011–1031.
- Zhang, L. (2011). Advertising in a new age of media. *China Business Review*, 38(1), 16–20.
- Zhu, Y. (2006, January 16). Web users worry about ease of obtaining personal data. *China Daily*, p. 4.
- Zhuge, Ji., Gu, L., Duan, H., & Roberts, T. (2015). Investigating the Chinese online underground economy. In J. R. Lindsay, T. M. Cheung, & D. S. Reveron (Eds.), *China and cybersecurity: Espionage, strategy, and politics in the digital domain* (pp. 87–120). New York, NY: Oxford University Press.

About the Author



Dong Han is currently Assistant Professor in the School of Journalism, Southern Illinois University Carbondale, Carbondale, USA. He has a PhD in Communications from the University of Illinois at Urbana-Champaign. He was legal counsel in China Central Television (CCTV) from 1999 to 2004. Dong Han has published with the *International Journal of Communication, Television and New Media, Global Media and Communication, Chinese Journal of Communication*, and *Ethnic and Racial Studies*.