International Journal of Communication 12(2018), 3877–3895 1932–8036/20180005

# Asymmetrical Power Between Internet Giants and Users in China

AOFEI LV[1]
University of Amsterdam, The Netherlands

TING LUO
Leiden University, The Netherlands

We find that the asymmetry of power between the Internet giants and the users, prevalent in the digital era, is deeply problematic in China in that the two key players of big data—the Internet giants and the government—are interested in exploiting the potential of big data, but the regulation of the use and application of user data is an obstacle to their goal. The Internet giants do not value the provision of transparent privacy policies and the enforcement of the policies, while the government, being an investor in and consumer of big data services, is neither interested in nor technologically capable of regulating big data technology. Moreover, there is no unified Internet governance system to solicit cooperation within the government to regulate Internet privacy. These contextual characteristics facilitate the building of the social credit system that pays limited attention to user privacy. The findings suggest that in the discussion about the political consequences of ICT development in China, we should focus on the Internet giants and their unchecked technological power instead of only the government.

*Keywords: big data, Chinese Internet giants, Internet privacy, social credit system*

The recent Cambridge Analytica scandal—which involved the use and application of data from up to 87 million Facebook users in political campaigns without their explicit consent—has vividly demonstrated the political power of the Internet companies with big data technology ("Cambridge Analytica," 2018). The scandal has made people in Western liberal democracies aware of the risks posed to the public when the Internet companies grow too powerful because of their access to and application of

Aofei Lv: A.Lu@uva.nl
Ting Luo: t.luo@fsw.leidenuniv.nl
Date submitted: 2017–12–07

[1]This research was supported by the project "Authoritarianism in a Global Age" at the University of Amsterdam (http://www.authoritarianism-global.uva.nl/) and received funding from the European Research Council (Grant No. 323899). For insightful comments and suggestions for revisions, we would like to thank the editors of this journal, the two anonymous reviewers, Jane Duckett, Marlies Glasius, and Marcus Michaelsen. We also thank Zhu Xufeng and Liang Zheng for their support at the China Institute for Science and Technology Policy, Tsinghua University, during the fieldwork.

big data. Yet, while discussing the political impact of ICT in China, scholars and observers tend to focus predominantly on the role of the government in using the big data technology for censorship and surveillance and overlook the power of the Internet giants in China that own and apply the ICT.

The power of the Internet giants comes from their collection, storage, and use of user data. The growing popularity of Internet services in China in recent years has provided the Internet giants with a tremendous amount of user data, making them as powerful as their Western counterparts, if not more so. As of December 2017, the Internet penetration rate in China was 55.8%, more than the global average of 51.7%. Of the 772 million Internet users in China, 93.3% use instant messengers, 68.8% use smartphone payments instead of cash or bank cards for offline purchasing, 69.1% use e-commerce, and 44% use WeChat or Alipay for e-government services, such as social insurance, health insurance, tax, public transportation, and utility bills (CNNIC, 2018). In this article, we illustrate the unregulated collection, usage, and application of user data by the Internet giants and explain why this poses risks to the rights of the users who produce the data.

What risks can the use and application of big data by the Internet giants pose to the users? While people enjoy the convenience facilitated by the Internet giants, and these giants enjoy ever-growing power and profits, few are aware of the potential privacy threats that Internet giants' collection and analysis of personal information pose to Chinese citizens. The notion of privacy indicates one's interpersonal boundary-control processes (Altman, 1975). However, as our social, communicative, and commercial acts increasingly take place online, we leave digital records that are stored by and accessible to Internet giants (Tufekci, 2008). The privacy threats arise when digital records are controlled and used by the Internet giants, and users are no longer able to control their privacy.

Furthermore, with ICT development, the Internet giants are empowered with various tools, such as data mining, association rule learning, and a priori algorithms (e.g., Fayyad, Piatetsky-Shapiro, & Smyth, 1996; Puschmann & Burgess, 2014). With these tools, the giants can not only analyze user data, but also manipulate and filter information for commercial gains. This creates an asymmetry of power between the Internet giants who collect and use the data, and the users who produce the data. Access to user data and big data technology allows Internet giants to decide users' access to information and knowledge, which affects people's real-life choices. Although the asymmetrical power between Internet companies and users is prevalent in the digital age, we argue in this article that the problem is deeply problematic in China.

Relying on interviews with 29 ICT experts, social science scholars, and government officials,[2] we focus on two key players of big data technology—the Internet giants and the government—and examine the contextual characteristics in China that have allowed the giants to exploit user data with very limited restrictions, aggravating the asymmetry of power between Internet giants and users. We find that on ICT development, the government and the Internet giants are currently allies; ICT development can sustain economic growth and technology development for the government, and bring revenues to the Internet

[2] The semi–structured interviews were conducted between October 2015 and June 2016 in Beijing, Shanghai, Hangzhou, and Shanxi.

giants. Thus, at present, both the Internet giants and the government have limited interest in regulating Internet privacy. Moreover, the government also lacks the technological capability and a unified Internet governance system to regulate Internet privacy. These contextual characteristics facilitate the building of the social credit system that pays limited attention to user privacy.

Regarding case selection, we choose Baidu, Alibaba and Tencent (BAT)—the biggest Chinese Internet giants—as the main cases of the Internet giants in China for two reasons. First, they are not only the largest Internet service providers in terms of annual profits and the number of active users in China, but also the most important digital players of the Chinese economy and ICT development. BAT are three of the world's top 10 largest Internet corporations in terms of revenue and market capitalization. By the end of 2017, the market capitalization of BAT took 73.9% of total market capitalization of Chinese-listed Internet companies (CNNIC, 2018). Moreover, BAT not only develop their own technology, but also invest in ICT development. In 2016, BAT provided 42% of all venture capital investment in China. In comparison, Facebook, Amazon, Netflix, and Google together contributed 5% of venture capital investment in the United States in the same year. One in every five top Chinese start-ups is founded by BAT, and an additional 30% of them receive funding from BAT (Woetzel et al., 2017).

Second, the ability of the Internet giants to collect, use, and apply big data depends on their business model. And the business model of BAT—attracting users to stay on their platforms for every aspect of their lives—enables BAT to collect user data covering all areas of online and offline activities and to build a large user base for the use and application of big data. This serves the research purpose of this article: investigation of the unregulated use of user data by Internet companies in China. Unlike the Internet corporations in the United States that tend to specialize in a few core businesses—for example, Twitter in microblogging and Uber in ride sharing—BAT are expanding their businesses vertically and horizontally into various areas that closely link both online business and offline local services, and they offer users a one-stop shop for a wide variety of services, including health, information, entertainment, e-commerce, and social interactions. This creates a multifaceted and multi-industry digital ecosystem (Jia & Kenney, 2016). As such, the Chinese are increasingly reliant on these all-in-one super-apps for managing their daily activities, enabling BAT to have access to tens of millions of pieces of user data.

This article proceeds as follows. We begin with a review of literature on the power of ICT in China and outline the contributions of this article, followed by an examination of the asymmetrical power between Internet companies and users in the digital era. In the fourth section, we provide empirical evidence to illustrate the practices of information manipulation and filtering conducted by the Internet giants in China. Then, we examine the four contextual characteristics in China that have aggravated the digital divide between Internet giants and users, and the building of the social credit system is used as an example to illustrate these contextual characteristics. Finally, the article concludes with implications and avenues for future research.

## The Power of Information Communication Technologies in China

As ICT and the Internet have become important communication tools, scholars have acknowledged the political impact of ICT on the state and the citizens in China. Earlier scholarship has

emphasized the efforts by the Chinese government to develop online censorship techniques. In China, an extensive system of Internet surveillance and control has been built to control information flow. The system includes the building of a government-controlled gateway to channel international connections to the global Internet (Boas, 2006), the regulation of privately owned and operated Internet platforms and telecommunications networks (Mackinnon, 2011), and the construction of a hierarchical structure of Internet regulation and a system of punishment mechanisms directed at various actors in the networks (Qiu, 2000).

Increasingly, the Chinese government has moved toward adopting softer and subtler methods of online control. The government hires online troops to fabricate support and distract attention away from controversial issues (Han, 2015; King, Pan, & Roberts, 2017; Miller, 2016). Online space has also been used by party officials to gather information about public opinion (Qiang, 2011), to receive feedback on policies and respond to public opinion strategically (Chen, Pan, & Xu, 2016), and to inform official media or identify and neutralize potential threats (Sullivan, 2013).

Although much of the current discussion on the power of ICT in China has concentrated on the use of ICT for informational and communicative activities, and how the informational and communicative functions of ICT empower the government, here we consider the commercial function of ICT as well as the other two functions in our analysis of the power and political impact of BAT. This shift of focus is particularly relevant to the development of ICT and the new trend that people are increasingly using the Internet not only for informational and communicative activities, but also for commercial activities—purchasing products online, for example. This is the first contribution of the article.

The second contribution is to shift the current discussion on the power of ICT in China from the government to the Internet giants. Thus far, the discussion has focused on the former, especially its ability to co-opt the Internet giants for surveillance and censorship. Yet, the relatively powerful interests in the use and application of big data include not only the government, but also Internet giants who have direct access to and control of the big data. We know very little about the power of the Internet giants in China and its impact on Internet users.

## The Asymmetrical Power Between Internet Companies and Users in the Digital Age

Though there is limited discussion on the asymmetry of power between Internet companies and users in China, the impact of the application of big data on users has been widely discussed by communication scholars in other contexts. Big data refers to a capacity to search, aggregate, store, and cross-reference large data sets (boyd & Crawford, 2012). There are three specific characteristics of big data—the amount of data, the speed of data, and the range of data types/sources—that require advanced technical approaches and skills to store and make use of it (Curry, 2016). These challenges create a digital divide between the big data rich and the big data poor (boyd & Crawford, 2012). More specifically, the digital divide represents the asymmetrical power between the relatively small group of privileged companies that have the means to collect data and the expertise to analyze data, and the large group of Internet users who create the data (Manovich,

2012). The threat to user privacy and the asymmetrical power between Internet companies and users is exacerbated by the companies' application of data mining, data sorting, and targeting.

In the data mining process, the digital divide mainly concerns access to information, data, and technology. Data mining is the process of surveilling data and discerning unexpected and unanticipated correlations behind the massive amount of human online activities (Andrejevic, 2014). There are two problems behind data mining. First, it involves surveillance and monitoring of citizens' online data. The boundary between surveillance for a government's political purposes and surveillance for commercial purposes is blurred in that any government can also be a customer of the Internet companies and purchase the surveillance and monitoring services. Snowden's revelations have shown that government agencies in Western liberal democracies are also mining and digging into data that users share with the commercial Internet companies (Greenwald, 2014). As Garton-Ash concluded (2013), "were Big Brother to come back in the 21st century, he would return as a public-private partnership" (2013, para. 1). Second, interpretation is an essential element of data analysis, which is subject to limitation and bias (boyd & Crawford, 2012). With the Internet giants dominating the mining and analyzing of user data, the analysis and interpretation of the human online data might well be biased toward the interests and viewpoints of the privileged Internet companies, and disempower the users.

In the data sorting and targeting process, the digital divide goes beyond access to data and technology, concerning access to useful knowledge and impacting people's life choices (Andrejevic, 2014; Lyon, 2003). Data sorting and targeting is a process of creating and reinforcing social divisions or even digital discrimination (Lyon, 2003). Raw data are sorted based on a set of criteria decided by and only known to the Internet companies; based on classified information, Internet companies can predict user preferences and feed users with information they think those users want. This personalization process creates the so-called filter bubble, which can introduce a new form of invisible propaganda, indoctrinating users with their own ideas and amplifying users' desire for things that they are familiar with (Pariser, 2011). This new form of invisible propaganda can be used by governments for political purposes and by commercial corporations for commercial purposes. Because of personalization, the effect of propaganda might be more persuasive because it appears subtler and less artificial.

In sorting and targeting, based on probabilistic predictions that take into account both individual and aggregate level data over time, the Internet companies decide who gets access to what knowledge or information in what form. Moreover, in the process of selecting information, governments or commercial corporations can purchase influence. Thus, the asymmetry runs deep in that it creates "a divide between the kinds of useful 'knowledge' available to those with and without access to the database" (Andrejevic, 2014, p. 1677), and it can have real effects on people's life chances (Lyon, 2003).

Next, we explain the practices of information manipulation and filtering by the Internet giants in China that create the asymmetry of power between the giants and the users.

**Information Manipulation and Filtering by the Internet Giants in China**

Similar to their Western counterparts, Internet giants in China manipulate and filter information and create the "filter bubble." One typical example is the customized news delivery by online news aggregators. Jinri Toutiao is a very popular online news aggregator in China. As an engineer of big data in Baidu revealed:

> Jinri Toutiao claims to be an intelligent news portal that selects and feeds news to users based on user needs. Counting on Jinri Toutiao to select and feed news means that users transfer their rights of information selection to the app. As long as you use the app to read news, it will always select what it wants you to see. For instance, Jinri Toutiao always puts official propaganda news of President Xi at the top of the news list. Did you choose to read it? No! That is because it wants you to see it. [3]

In this case, the political intention of the government is featured in the personalization of news information.

The sorting and targeting of information can also be affected by commercial purposes. Deleting negative news and information about a brand is a typical marketing strategy in the digital marketing field. Depending on the difficulty of deletion and the popularity of social media sites, the price of deleting negative information ranges from $15 (¥100) to $750 (¥5000) per post (Wu, Jakubowicz, & Cao, 2014). Censoring negative information is quite often requested by celebrities and companies to cover up negative news that can influence their reputation or stock prices. A senior manager of a private Internet company provided an example:

> Social media are able to arrange the content in the way they want. Otherwise how could those celebrities, officials, and companies cover up their scandals, such as cheating, corruption, and other negative news? A few months ago, when pictures showing that XXX [a Chinese movie star] cheated on his wife was exposed on the Internet, do you know how much he paid for Weibo to cover up and how much he paid for online troops to "clean" him? . . . We didn't delete all the discussions of this issue, because it takes too much effort. We just disabled any "#" related to this so it wouldn't be promoted to the front page as a "hot topic." In the meantime, we promoted other news, such as soccer and Adele's new songs. Eventually, public attention shifted, because people forget things very easily. We use the same technical methods to deal with any information requested by a third party.[4]

In this case, information is covered up, and the commercial online troops are hired to fabricate support and distract attention away from the negative information for commercial companies and

[3] Interview with B003, engineer of big data, Baidu, May 2017, telephone.

[4] Interview with A015, senior manager of government relations, Youku, January 2016, Beijing.

celebrities. The 50 cent parties documented by political science scholars (Han, 2015; King et al., 2017; Miller, 2016) do not seem to differ much from the commercial online troops in this example.

On search engines, companies can pay to have their results ranked high in the search results. Baidu sells the listings to bidders (*jingjia paiming*) who pay the highest prices, without vetting the claims or products. As a Baidu manager revealed, "Our main task is to earn profit for Baidu. We don't have authority or expertise to judge whether the ads are real or not."[5] False claims made by a hospital appearing on a Baidu search result, for example, indirectly caused the death of a young college student in China ("China Investigates," 2016). Although this is an extreme case, given that people are increasingly relying on the Internet to acquire information, the selection of "useful" information by the Internet companies has tremendous impact on people's real-life decisions.

Although the asymmetry of power between the Internet giants and the users in China presented earlier does not differ much from the same conflict in developed, Western countries, we will demonstrate next why the privacy risks posed by the Internet giants' application of big data are worse in China. Existing scholarship on privacy concerns tends to paint China as an exceptional case where, for historical and cultural reasons, the public lacks privacy concerns (Farrall, 2008; McDougall & Hansson, 2002). Yet, empirical investigations reveal that Chinese Internet users are not much different from users elsewhere in the world regarding the relationship between privacy concerns and information disclosure online. Studies of users of social network sites, such as Facebook and Myspace, found no association between privacy concerns and users' decision to join Facebook and to reveal personal information (Acquisti & Gross, 2006; Tufekci, 2008). Similarly, a survey study of Weibo users in China reveals that information disclosure is strongly related to user perception of benefits they can gain from the online media, while it has no association with their privacy concerns (Zhang, Amos, & Pentina, 2015). Therefore, public perception of privacy is not the reason for the aggravated Internet privacy violations in China.

Instead, we focus on the two key players of big data in China—the Internet giants and the government—and examine the contextual characteristics that have allowed the exploitation of user data. We start by looking at the lack of transparent privacy policies and enforcement of the policies by the Internet giants.

### The Lack of Transparent Privacy Policies and the Enforcement of the Policies

Although popular websites were launched in China in the early 2000s, the first national assessment of privacy policies of Internet products and services was carried out and released more than a decade later, in 2017. This annual report illustrated the prevalence of poor transparency in the privacy policies of websites and apps in China (Nandu Personal Data Protection Research Centre, 2017). In their assessment of the privacy policies of the most popular 1,550 Chinese websites and apps, more than 80% ranked low or relatively low in privacy policy transparency. Common problems in the "low" or "relatively low" ranks are a lack of user rights clauses, the use of standardized and older versions of privacy texts that fail to reflect the services provided or to protect users' rights, and having terms that allow Internet

[5] Interview with B012, senior product manager, Leshi, June 2017, Beijing.

giants to sell user data for commercial purposes without asking for user consent. What is worse, a few websites and apps do not have any privacy policies.

The assessment concerns only the contents of privacy policies. Yet, to deal with the threat to user privacy, the implementation and enforcement of privacy policies are much more important. As the annual report has noted, how Internet giants implement their privacy policies, especially on issues such as how to share user information with third parties and how to deal with user data of unregistered users, remains unknown.

Installing mechanisms to regulate and enforce the collection, storage, and use of user data is not a concern of the Chinese Internet giants. In March 2018, in a discussion about user privacy at a China development forum with the CEOs of IBM and Google, Baidu CEO Robin Li claimed that Chinese users are less concerned about privacy and more willing to trade personal privacy for the greater convenience offered by Internet services and products than users in the West (The Beijing News, 2018). This claim triggered a heated debate online and received a lot of criticism from Internet users in China, demonstrating that the claim was no more than an excuse used by the Internet giants to justify their lack of user privacy protection policies. For the majority of Internet giants in China, their priority is to collect as much user data as possible and decide later what data to use and how (Yang, 2018).

**Lack of Government Interest in Regulating Internet Privacy**

The most important factor exacerbating the abuse of user data by Internet giants is the lack of government interest in regulating their access to, management of, and use of user data. The Chinese government is an investor and consumer of big data services—and the government's interests lie in exploiting the potential of big data rather than regulating it. A report by McKinsey on digital development in China noted, "The government gave digital players space to experiment before enacting official regulation, and is now becoming an active supporter" (Woetzel et al., 2017, p. 13). During the early stage of Internet development, digital players did enjoy considerable space for development and innovation. For instance, the first online payment service was launched by Taobao (Alibaba's e-commerce website) in 2003, and it was not until 2010 that The People's Bank of China started to regulate it through the first regulation, "Non-financial Institutions Payment Service Management Measures" (The People's Bank of China, 2010). Consequently, between 2003 and 2010, Taobao had considerable leeway to develop its e-commerce business, collect user data, and use the data to innovate its payment services (Woetzel et al., 2017). A previous Ministry of Information and Information Technology (MIIT) officer also attributed the wild growth and expansion of the Chinese Internet companies in the first decade of the 21st century to the fact that the government imposes very limited restrictions on the digital players.[6]

Today, the government has become an active supporter of digital players by promoting the digital economy and ICT development. A series of policies have been issued to develop and strengthen ICT as a new engine for economic growth. For instance, in 2015, the government unveiled a national development plan, "Internet Plus," the key of which is to keep pace with the information trend and utilize Internet

[6] Interview with A009, CEO of a fintech company, then an official of the MIIT, and then senior manager of government relations, Baidu, November 2015, Beijing.

development to boost economic development (State Council, 2015). The development plan came with a series of detailed action plans that integrate the Internet, cloud computing, big data, logistics, social security, consumer industry, and manufacturing. In 2017, China Internet Investment Fund, a state-owned venture capital fund, planned to invest $15.89 billion (¥100 billion) in Chinese Internet companies (Woetzel et al., 2017). As can be seen, the Chinese government's priorities and interests lie in helping Internet giants to develop digital technology for economic growth—and ICT development relies on the collection, storage, and use of user data. Thus, there is little incentive for the government to rein in the use and application of big data for the sake of user privacy.

The Chinese government's lack of interest in protecting user privacy is also illustrated by actions taken by responsible ministries and party organs. For example, in September 2010, Qihoo360, the biggest Chinese Internet security company known for its antivirus software, accused QQ, an instant messenger from Tencent, of spying on and scanning its users' computers for personal data. Tencent fought back and accused Qihoo360 of fabricated news and illicit competition. Although part of the dispute was related to the collection and use of users' personal information, the MIIT, which is directly in charge of Internet development, only intervened in the dispute in regard to illicit market competition. The solution provided by MIIT in November 2010 solely focused on how to regulate the competition between the two companies, but made no mention of how to protect user privacy (MIIT, 2010).

This reveals the government's interest in ICT development, which it considers a new engine for sustainable economic growth. Allowing the Chinese Internet giants to explore the potential of big data technology is key to this vision. Thus, as it stands, the Chinese government is unlikely to regulate Internet privacy for the sake of user personal information security because this would stifle the growth of Internet giants in China.

### The Chinese Government's Lack of Technological Capability

That the Chinese government has been successful in soliciting the cooperation of the Internet giants in developing and applying ICT for censorship and surveillance has made scholars and observers overestimate the government's technological capability. As we will show, it is the Internet corporations that build the Internet tools and develop big data and algorithms; it is also the corporations that execute and implement censorship and surveillance on behalf of the Chinese government. The government does not have the skills in and knowledge on big data, or the working manner and mindset, to develop and manage such data, preventing it from regulating the big data use of the Internet giants. In other words, the Chinese government lacks the technological capability to regulate big data technology.

Realizing the importance of big data and the information industry, the Chinese government has built a few big data centers, such as the Guiyang Platform for Big Data Transaction Services (built in April 2015). Government departments and state-owned corporations also sponsor or create state-led institutions and projects for big data research, such as the Beijing Institute of Big Data Research. Yet, the building of these institutes and projects is often only to please higher-level government and to receive government funding. Staff working in these state-led or state-owned centers have neither skills in nor

knowledge on big data. The Guiyang big data center is a typical example. An engineer of a state-owned telecom corporation revealed:

> Do you know how my company decided to build the big data research center? When President Xi visited Guiyang center [Guiyang platform for Big Data Transaction Services], he said "Big data is really important." The executive of my company saw it as an opportunity to join a project strongly promoted by the government, especially since "Internet Plus" is such a hot concept. He then applied for government funding to build the big data center. That's it! It is not because my company has the capability to collect big data or analyze it, or has a detailed plan to develop big data technology. It is just because it's a government-led project and my company wants to share some profit. … Moreover, the center is now led by officials appointed by upper-level leaders instead of engineers. How could a political official analyze big data? As an engineer, it is difficult for me to explain to them what big data is, to say nothing about the complicated computer technology.[7]

Because of a lack of skills in and knowledge on big data technology, the Guiyang big data center has ended up being primarily a center for storing big data, with limited data storage capacity.

Another major problem faced by the state-owned or state-led data centers is the bureaucratic mindset and manner of working. In these data centers, staff strive to follow orders from above instead of focusing on developing technology and innovating big data analysis to satisfy user needs. That the Guiyang center was built to attract funding from the government has also vividly demonstrated this problem. A senior engineer of the Chinese Academy of Sciences revealed the difference between the Internet giants and the government in terms of developing and managing big data technology:

> Compared with BAT, state-owned companies and data centers do not base the development of technology on market demands, and they also do not have the capability to apply technology in practice. If you check the programs of all conferences on advanced technology in China, you will find that most advanced technology is developed by BAT. In other words, BAT are far more advanced than the state-owned companies and the Chinese Academy of Sciences on technology development. [8]

As can be seen, the Chinese government does not have the skills in and knowledge on big data, or the working manner and mindset, to develop and manage big data. This weakness has prevented the government from regulating the use and application of big data. The technological know-how for big data technology is predominantly possessed by the Internet giants. The Chinese government has the big data vision, but does not have the skills, knowledge, or mindset. The example of real name registration

[7] Interview with B009, engineer of a state-owned telecom company, June 2017, Taiyuan.

[8] Interview with B011, senior engineer of the Chinese Academy of Sciences, then engineer of Huawei, June 2017, Beijing.

illustrates the difference between the government and the Internet giants in their technological capability. An engineer of big data at Sohu revealed:

> Ten years ago, when the Chinese government started to call for real name registration on the Internet, people were reluctant to do it. However, nowadays when Ali or WeChat says "register with your real name, you will get a bonus or have access to advanced functions of the apps," people are eager to do so voluntarily. You tell me which is more powerful: the government or the companies.[9]

This example demonstrates that using ICT, the Internet giants are able to incentivize users and achieve real-name registration on the Internet, whereas the government cannot.

**Fragmented Internet Governance System**

Fragmentation of Internet governance within the central government and across different regions and areas of China makes it difficult to build collaboration on Internet privacy regulation and is another major obstacle to a unified effort on big data regulation. At the central level, departments are assigned different and conflicting responsibilities related to the Internet, making it difficult for them to cooperate on Internet privacy regulation. The Cyberspace Administration of China (CAC),[10] headed by the CCP General Secretary Xi Jinping, is in charge of censorship, oversight, and regulation formulation and implementation on a variety of issues related to the Chinese Internet, while the State Council and its department, the MIIT, is in charge of Internet development, such as infrastructure, business registration, and technological development. The government wants to boost economic development by promoting Internet development on the one hand, but wants to maintain stability by controlling information on the Internet on the other (Lee & Lio, 2016). Quite often, these two aims are conflicting, but they are assigned to these two organizations at the central level, with the CAC responsible for maintaining stability and the State Council responsible for economic development. The disagreement between these two organs at the central level regarding their aims makes it difficult for them to cooperate on regulating Internet privacy.

Even though the CAC has grown considerable enforcement power since 2014, regulating Internet privacy is not its priority. Since 2014, the CAC has been centralizing power on various issues related to the Chinese Internet from other departments, including taking away the enforcement power possessed by the MIIT. However, the CAC's priority lies in censoring contents on the Chinese Internet. For instance, in July 2016, the CAC closed some news programs on Tencent and other news sites because of the publication of a large amount of independently gathered news reports (Beijing Times, 2016). In September 2017, the CAC fined Tencent, Baidu, and Weibo for hosting fake news, pornography and other forms of banned content (CAC Beijing City Branch, 2017). When it comes to violation of user privacy, Internet giants only receive warnings from the MIIT. For example, in January 2018, the MIIT warned

[9] Interview with B014, engineer of big data at Sohu, June 2017, Beijing.

[10] The CAC is also known as the Office of the Central Leading Group for Cyberspace Affairs and directly answers to the Central Leading Group for Internet Security and Informatization. Founded in 2014, it is the central Internet control agency in China.

Baidu, Ant Finance (a personal financial investment management APP), and Jinri Toutiao for their inadequate provision of data privacy measures to protect users' privacy.

The conflict of responsibilities and interests is further exacerbated downward to the local levels, making it hard for local governments to cooperate on Internet privacy regulation. Whereas central governments want to ensure compliance with their orders, local governments want to maximize the benefits they receive from their administration in the local areas (Egorov & Sonin, 2011). For example, the disagreement between central and local governments has impeded the building of a website that displays credits for all companies instructed by the State Council. The website requires sharing of companies' information online by different levels of governments. However, this information is crucial for local governments to bargain for political and economic resources. A senior manager of government relations at Baidu revealed:

> This project has been going on for years, but it is still underdeveloped because some departments refuse to take part. The departments use the information to argue for financial and personnel resources, so they have to hold the information exclusively.[11]

The development of e-governance demonstrates the fragmentation across different areas of China. The unequal Internet development across different areas and the different motives of local government officials make it impossible to build a comprehensive and universal e-governance system. As a CEO of a private Internet company revealed:

> Some counties in western China do not even have automatic office systems, while in some big cities like Beijing, Shanghai, and Shenzhen, people can almost do everything online. In some areas, e-governance is a priority of the local government. In these areas, even though the officials may not necessarily understand big data projects, they do it because of top-down orders or as a chance to apply for grants from upper level governments. In some other areas, the officials don't take e-governance or big data seriously, so they don't have the intention to build or use it. Some officials don't know what they need from the system, so it is difficult for us to design and build it.[12]

As can be seen, the fragmentation of Internet governance in Beijing and across different areas and regions in terms of interests and responsibilities has impeded collaboration within the government on Internet privacy regulation.

## The Social Credit System and Chinese Internet Giants

The building of the social credit system is a typical example that reflects the role of Internet giants in big data application. China's social credit system is an information technology-driven ambition of the government, which aims to create a central repository of data on citizens and organizations for

[11] Interview with A004, senior manager of government relations at Baidu, October 2015, Beijing.
[12] Interview with B006, CEO of a government big data project contractor, May 2017, Hangzhou.

monitoring, assessing, and changing their actions through carrots and sticks (Ohlberg, Ahmed, & Lang, 2017). It has been criticized by some Western observers and scholars for its potential to be used for political control. As some have claimed, the alliance of profit-driven private Internet companies with technological know-how and an authoritarian government could make the social credit system an effective tool for "Big Brother" to make compliant and patriotic citizens and prevent opposition (Clover, 2016). Yet, from the preceding discussion, we can see that while the Chinese government is a consumer of and investor in big data, the Internet giants have their own interests and privileged technology to address some profound social and economic problems via the social credit system. This has been neglected in the current discussion on the Chinese social credit system.

From the perspective of the Internet giants, they are building the social credit system for their commercial interests. A senior manager of Alibaba research noted that there were some major problems in the Chinese banking system: limited traceable credit record of individuals and companies stored, excessive bank transaction and administration fees, and the low penetration of bank card payment services. "We [Alibaba] are just trying to fill in those gaps."[13] In other words, the building of a social credit system is to address and solve these major problems in China's banking system and to achieve revenue for the Internet giants.

An important reason for assigning a social credit rating to every citizen is to build an inclusive finance system that will provide financial support, including loans to individuals from lower social classes and to small companies for business development. Small and medium companies in China, for example, either have no access to financial support from traditional banks or have to pay higher costs to obtain a loan. An interviewee explained how the social credit system could include individuals and companies deprived of access to financial support:

> When we try to give loans to small and medium companies, for example, we have no place to check their credit system and financial records; even if banks have the records, they refuse to share the information with us. . . . Thus, before the government authorized eight Internet companies to build a social credit system, we [Alibaba] had already noticed the strong demand to build our own credit system based on our user data and algorithms. Our intention is to build an individual's credit history based on their expenditure, rather than income, because we can rely on our e-commerce platform to gather their consumption history. In this way, we also do not need to rely on the banking system to collaborate with us and provide us with information.[14]

However, in the building of a social credit system, the government and the Internet giants have different expectations. The government intends to first allow Internet giants to pilot rating schemes and then merge these pilot rating schemes and the data into a comprehensive central-level system (Hornby, 2017). Currently, every Internet giant is experimenting with what it can do technically with its data and algorithms with limited restrictions. "If the regulation does not explicitly state that doing something is

[13] Interview with A017, senior manager of Alibaba Research, Alibaba, January 2016, Beijing.
[14] Interview with A017, senior manager of Alibaba Research, Alibaba, January 2016, Beijing.

illegal, then it is legal for us to do it."[15] This is precisely the current status of the regulation of the social credit system in China. There is no explicit restriction on how the Internet giants apply user data in building the social credit system, and thus they have space to push the boundaries of big data technology.

According to a senior manager of Alibaba, building this comprehensive central-level repository of data is not the Internet giants' intention. Rather, their intention is to have several companies offering different credit systems and providing users with choices.[16] As can be seen, the government relies heavily on the Internet giants' technological know-how to build such a comprehensive state-owned credit system, and it is not in the Internet giants' interest to build one system and transfer the ownership to the government. Because of the reluctance of the Internet giants to share data with rival platforms, the People's Bank of China decided not to issue any more licenses for the social credit system pilot in 2017 (Hornby, 2017).

Furthermore, it is also practically difficult to merge data from different Internet companies into one platform. As a CEO of a government big data project contractor explains:

> Different Internet companies hold different types of data, because they collect data in different ways. Therefore, with the current technology, it is practically difficult to merge all data from different companies into one platform. Even if people did it, it would be difficult to use the data. [17]

It is too early to speculate on the potential of the government to use such a system for political control. Conversely, in the commercial version of the social credit system envisioned by the Internet giants, they have the potential to make users enormously dependent on the products and services they offer, despite the lack of transparent privacy policies. Thus, the most prominent problem of China's social credit system(s) is the asymmetry of power between the Internet giants and the users, instead of the "Big Brother" problem, as is believed.

The preceding analysis demonstrates the following key points. First, the Internet giants' access to technology and data makes them indispensable digital players in the building of the social credit system. Second, the Internet giants' lack of (enforcement of) transparent privacy policies and the lack of government interest in and capacity to regulate Internet privacy make it unlikely that there will be mechanisms built in to deal with data privacy risks. Third, given that the Chinese government relies on the Internet giants' technological know-how to build the system, and the technological obstacles of merging different data into one central repository, it is too early to speculate and worry about the potential of the government to use such a system for political control. But, with limited regulation on the use and application of big data, the privileged access to and control of big data technology does provide the Internet giants with considerable power to abuse user privacy and affect people's real-life chances, putting the users in an increasingly powerless position.

---

[15] Interview with B005, senior manager of government relations, Qihoo360, May 2017, Beijing.
[16] Interview with B005, senior manager of government relations, Qihoo360, May 2017, Beijing.
[17] Interview with B006, CEO of a government big data project contractor, May 2017, Hangzhou.

## Conclusion

We find that, similar to Google and Facebook, the Internet giants in China also filter information and decide who gets access to what knowledge or information in what form, creating the "filter bubble." The asymmetry of power between the Internet giants and the users is even worse in China in that the two key players of big data—the Internet giants and the government—are interested in exploiting the potential of big data, but regulation of the use of user data may be an obstacle to their goal. The Internet giants do not value the provision of transparent privacy policies and the enforcement of such policies, while the government, being an investor in and consumer of big data services, is neither interested in, nor technologically capable of, regulating big data technology. Moreover, there is no unified Internet governance system to solicit cooperation within the central government and across different regions and areas of China to regulate Internet privacy.

These contextual characteristics facilitate the building of a social credit system that pays little attention to Internet privacy. The case of the social credit system also demonstrates that the government relies on the Internet giants' technological know-how to build a government-owned central data system, but the Internet giants share a different vision of the social credit system—namely, they desire a privatized credit system that offers users choices. The technical barriers to merging data collected by different companies and government organs into one system and standardizing them also pose great obstacles to building the central system envisioned by the government. Thus, it is too early to worry about the "Big Brother" problem; the more prominent problem of the social credit system(s) is the widening digital divide between the Internet giants and users.

There are two important caveats in interpreting the findings of this article. First, we do not suggest that the "Big Brother" problem, commonly discussed by international observers and scholars, does not exist in China. The Chinese government can certainly use its political power to control the Internet giants if they become too technologically powerful. However, given that the Chinese government and the Internet giants are allies on economic and ICT development, it is unlikely that the government will strictly control the Internet giants through hard political means (e.g., shutting them down). Second, though we do not preclude the possibility of future regulation of Internet privacy by the Chinese government—with a change of interest, technological capability, and governance system—we have focused our analysis on the current stage of ICT development. We find that the protection of user privacy in the collection, storage, analysis, and usage of user data, which would impede the exploration of big data potential, is currently of concern to neither the government nor the Internet giants.

Finally, our findings also have important implications for the discussion about the political consequences of ICT development and the power of Internet giants. With the Internet giants' growing user base in China, and the contextual characteristics providing a relatively free environment for the collection and usage of user data, the giants may become even more powerful than their Western counterparts. People in the United States have already started to be aware of the potential of tech giants to be the new political power in Washington, while neither scholars nor the general public have paid sufficient attention to the potential of the Chinese Internet giants to be influential in the political arena (Solon & Siddiqui, 2017). Future studies could probe further into the power possessed by the Internet giants and their

impacts on society and the state. Beyond China, with the Chinese Internet giants' global expansion and entry into the global market, research on their interaction with the government and the citizens of the countries where they set up new businesses can certainly shed light on the tech giants' political and social impact across the planet.

## References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In P. Golle & G. Danezis (Eds.), *Proceedings of the 6th workshop on privacy enhancing technologies* (pp. 36–58). Cambridge, UK: Robinson College.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole.

Andrejevic, M. (2014). The big data divide. *International Journal of Communication, 8*, 1673–1689.

The Beijing News. (2018). Baidu's two apps access users' information without their consent [Baiduxi liangkuan APP weijing tishi kaiqi yinsi quanxian]. *Xinhua News Agency*. Retrieved from http://www.xinhuanet.com/fortune/2018-03/28/c_1122600485.htm

Beijing Times. (2016). Some websites are shut down for illegal report. *Renminwang*. Retrieved from http://society.people.com.cn/n1/2016/0725/c1008-28580811.html

Boas, T. C. (2006). Weaving the authoritarian web: The control of Internet use in nondemocratic regimes. In J. Zysman & A. Newman (Eds.), *How revolutionary was the digital revolution? National responses, market transitions, and global technology* (pp. 361–378). Stanford, CA: Stanford Business Books.

boyd, d., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information Communication and Society*, *15*(5), 662–679. http://doi.org/10.1080/1369118X.2012.678878

CAC Beijing City Branch. (2017). Wangxin chufa weibo weixin tieba: dui weigui xinxi weijindao chuli yiwu [CAC penalised Baidu tieba for not strictly managing illegal content]. *Wangyi163*. Retrieved from http://news.163.com/17/0925/16/CV6M1SN00001899N.html

Cambridge Analytica: Facebook data-harvest firm to shut. (2018). *BBC*. Retrieved from http://www.bbc.com/news/business-43983958

Chen, J., Pan, J., & Xu, Y. (2016). Sources of authoritarian responsiveness: A field experiment in China. *American Journal of Political Science*, *60*(2), 383–400.

China investigates the search engine Baidu after student's death. (2016). *BBC*. Retrieved from http://www.bbc.com/news/business-36189252

Clover, C. (2016). China: When big data meets big brother. *Financial Times*. Retrieved from https://www.ft.com/content/b5b13a5e-b847-11e5-b151-8e15c9a029fb

CNNIC. (2018). *Di Sishiyici Zhongguo Hulian Wangluo Fazhan Zhuangkuang Tongji Baogao* [The 41st statistic report on the development of China's Internet]. *China Internet Network Information Center*，Beijing, China.

Curry, E. (2016). The big data value chain: Definitions, concepts, and the theoretical approaches. In J. M. Cavanillas, E. Curry, & W. Wahlster (Eds.), *New horizons for a data-driven economy: A roadmap for usage and exploitation of big data in Europe* (pp. 29–37). Berlin, Germany: Springer. http://doi.org/10.1007/978-3-319-21569-3

Egorov, G., & Sonin, K. (2011). Dictators and their viziers: Endogenizing the loyalty-competence trade-off. *Journal of the European Economic Association*, *9*(5), 903–930.

Farrall, K. N. (2008). Global privacy in flux: Illuminating privacy across cultures in China and the U.S. *International Journal of Communication*, *2*, 993–1030.

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI Magazine*, *17*(3), 37–54. http://doi.org/10.1145/240455.240463

Garton-Ash, T. (2013). If big brother came back, he'd be a public-private partnership. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2013/jun/27/big-brother-public-private-partnership-nsa

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. London, UK: Hamish Hamilton.

Han, R. (2015). Manufacturing consent in cyberspace: China's "fifty-cent army." *Journal of Current Chinese Affairs*, *44*(2), 105–134.

Hornby, L. (2017). China changes tack on "social credit" scheme plan. *Financial Times*. Retrieved from https://www.ft.com/content/f772a9ce-60c4-11e7-91a7-502f7ee26895

Jia, K., & Kenney, M. (2016). *Mobile Internet business models in China: Vertical hierarchies, horizontal conglomerates, or business groups* (BRIE Working Paper 2016-6). Retrieved from http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Working-Paper-2016-6.JiaKenney.pdf%0A

King, G., Pan, J., & Roberts, M. E. (2017). How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. *American Political Science Review*, *111*(3), 484–501.

Lee, M.-H., & Lio, M.-C. (2016). The impact of information and communication technology on public governance and corruption in China. *Information Development*, *32*(2), 127–141.

Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. London, UK: Routledge.

Mackinnon, R. (2011). China's "networked authoritarianism." *Journal of Democracy*, *22*(2), 32–46. doi:10.1353/jod.2011.0033

Manovich, L. (2012). Trending: The promises and the challenges of big social data. In M. K. Gold (Ed.), *Debates in the digital humanities*, (VI, 460-475). Minneapolis, MN: University of Minnesota Press. http://doi.org/10.5749/minnesota/9780816677948.003.0047

McDougall, B. S., & Hansson, A. (Eds.). (2002). *Chinese concepts of privacy* (Vol. 55 of Sinica Leidensia). Leiden, The Netherlands: Brill.

MIIT. (2010). *Guanyu piping beijing qihu keji youxian gongsi he shenzhen tengxun jisuanji xitong youxian gongside tongbao* [Criticism of Beijing Qihoo Technology Co., Ltd. and Shenzhen Tencent Computer System Co., Ltd.]. Retrieved from http://www.miit.gov.cn/n1278117/n1287041/n4312488/c4312593/content.html

Miller, B. (2016). *Automated detection of Chinese government astroturfers using network and social metadata.* Retrieved from SSRN: https://ssrn.com/abstract=2738325

Nandu Personal Data Protection Research Centre. (2017). *Annual report of privacy policy transparency*. Retrieved from http://www.dgcs-research.net/a/Opinion/2018/0310/126.html

Ohlberg, M., Ahmed, S., & Lang, B. (2017). *Central planning and local experiments: The complex implementation of China's Social Credit System*. Berlin, Germany: Merics.

Pariser, E. (2011). *The filter bubble: How the new personalized web is changing what we read and how we think*. New York, NY: Penguin.

The People's Bank of China. (2010). *Fei jinrong jigou zhifu guanli banfa* [Nonfinancial institutions payment service management measures]. Retrieved from http://www.pbc.gov.cn/tiaofasi/144941/144957/2845832/index.html

Puschmann, C., & Burgess, J. (2014). The politics of Twitter data. In K. Weller, A. Bruns, J. Burgess, C. Puschmann, & M. Mahr (Eds.), *Twitter and society* (pp. 43–54). New York, NY: Peter Lang.

Qiang, X. (2011). The battle for the Chinese Internet. *Journal of Democracy, 22*. http://doi.org/10.1353/jod.2011.0020

Qiu, J. L. (2000). Virtual censorship in China: Keeping the gate between the cyberspaces. *International Journal of Communications Law and Policy*, *4*, 1–25.

Solon, O., & Siddiqui, S. (2017). Forget Wall Street—Silicon Valley is the new political power in Washington. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/sep/03/silicon-valley-politics-lobbying-washington

State Council. (2015). *Guowuyuan guanyu jiji tuijin 'hualianwang+' xingdongde zhidao yijian* [Guiding opinions of the State Council on actively promoting the "Internet +" action]. Retrieved from http://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm

Sullivan, J. (2013). China's Weibo: Is faster different? *New Media & Society*, *16*(1), 24–37. http://doi.org/10.1177/1461444812472966

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20–36.

Woetzel, J., Seong, J., Wang, K. W., Manyika, J., Chui, M., & Wong, W. (2017). *China's digital economy: A leading global force*. Retrieved from https://www.mckinsey.com/featured-insights/china/chinas-digital-economy-a-leading-global-force

Wu, M., Jakubowicz, P., & Cao, C. (Eds.). (2014). *Internet mercenaries and viral marketing: The case of Chinese social media*. Hershey, PA: IGI Global. doi:10.4018/978-1-4666-4578-3

Yang, Y. (2018). China's Internet lenders fall foul of data privacy rules. *Financial Times*. Retrieved from https://www.ft.com/content/d21ca66a-2e2e-11e8-a34a-7e7563b0b0f4

Zhang, L., Amos, C., & Pentina, I. (2015). Information disclosure on a Chinese social media platform. *Journal of Information Privacy and Security*, *11*(1), 3–18. http://doi.org/10.1080/15536548.2015.1010981