Beijing Law Review
2013. Vol.4, No.1, 37-41
Published Online March 2013 in SciRes (http://www.scirp.org/journal/blr)
http://dx.doi.org/10.4236/blr.2013.41005

Regulating the Internet: China's Law and Practice*

Haiping Zheng
School of Law, Renmin University of China, Beijing, China
Email: haipingzheng@gmail.com

Received November 26th, 2012; revised December 27th, 2012; accepted January 4th, 2013

Though internet was not commercially available in China until 1995, it has been growing tremendously over the years. At the same time, the Chinese government has never ceased regulating or even censoring internet. This paper provides an overview of the development of internet in China, and the major regulatory schemes that have a direct impact on internet speech. Further, it describes some of the specific measures the Chinese government uses to control the internet: filtering and blocking, imposing liabilities on private parties, access control, internet "police", and "guiding" public opinion. Finally, it concludes that internet censorship does more harm than good.

Keywords: Internet; China; Freedom of Speech

Introduction

China's internet censorship has drawn much international criticism. For example, in 2006, the Reporters without Board included China as one of the 13 "enemies of the Internet" (Reporters without Borders, 2006). Then in 2010, Google decided to withdraw from Chinese market, claiming that Chinese government's attempts to limit free speech on the web, combined with other factors, had led the corporation to make such a decision (Official Google Blog, 2010).

On the other hand, the picture is not that gloomy. By 2008, the number of internet users in China has reached 220 million, making China the nation with the largest number of internet users. Furthermore, due to the very nature of internet, it is often difficult for the government to control the information transmitted through internet. Despite Chinese government's efforts to censor the internet, it is doubtful how much success it can achieve.

This paper examines China's internet censorship and its effects. Part 1 provides a general introduction to the development of internet in China. Such background information is necessary for the understanding and analysis of internet censorship in China. Part 2 introduces some of the regulations that have a direct impact on internet speech. Part 3 describes some specific measures (or techniques) the Chinese government utilizes to control the internet: filtering and blocking, imposing liabilities on private parties, access control, internet "police", and "guiding" public opinion. The final part is the conclusion of the paper.

Development of Internet in China

Although China began to be connected to the internet as early as 1987, internet was not commercially available in China until 1995. From then on, internet has been growing tremendously over the years. By 2008, infrastructure has extended broadband Internet access to 92 percent of townships (Zhao, 2008).

Like many other areas of China's economic development since 1978, development of internet was largely driven by the government. As a result, China's internet hardware infrastructure is highly centralized. Currently, there exist nine state-licensed Internet Access Providers (IAPs), each of which has at least one connection to a foreign Internet backbone. All the IAPs are required to be "at least fifty-one percent controlled by State-owned companies". These IAPs, in turn, grant regional Internet Service Providers (ISPs) access to backbone connections. All these entities (IAPs and ISPs) are required to register with the designated government agents. Those who fail to comply with the regulations face the threat of being shut down (ONI, 2005).

The government's monopolistic position in internet infrastructure facilitates censorship. Because all Internet traffic passes through the nine IAPs, the government can censor the information flow by adding filtering system "at the gateways." Moreover, as Part 3 will show, the government requires ICPs and ISPs to filter internet content, resulting in severe self-censorship.

International companies have been playing a significant role in the development and maintenance of China's internet infrastructure. The Cisco system, in particular, has been integral to China's Internet development. It specifically implemented the backbone networks for at least three of China's nine IAPs. Western corporations' such "conspiring" activities have been subjected to the criticism of human rights activists (Newbold, 2003).

Chinese Government's Attempts to Control the Internet: An Overview

Before the introduction of internet, the Chinese government, under the leadership of the Chinese Communist Party (CCP), essentially controlled all the traditional mass media, including newspapers, magazines, television, radio, etc. Unsurprisingly, the government sought to control the new media even before internet became commercially available. Over the years, the government promulgated numerous regulations to control the internet. This part provides an overview of the regulations that

*This article is one of the research results of the Project sponsored by China National Social Science Foundation (No. 12CFX020).

have a direct impact on internet speech.

On February 1, 1996, China's State Council promulgated the Interim Provisions Governing Management of Computer Information Networks. It prohibits four categories of information from being produced or transmitted online: information that would harm national security, disclose state secrets, threaten social stability or promote sexually suggestive material (art. 13).

On September 20, 2000, the State Council issued the Measures for Managing Internet Information Services (Measures, 2000), which significantly extended the scope of prohibited contents. Article 15 of the 2000 Measures provides:

ISPs (*internet service providers*) *shall not produce, reproduce, release, or disseminate information that contains any of the following*: 1) *Information that goes against the basic principles set in the Constitution*; 2) *Information that endangers national security, divulges state secrets, subverts the government, or undermines national unity*; 3) *Information that is detrimental to the honor and interests of the state* ⋯ 6) *Information that disseminates rumors, disturbs social order, or undermines social stability* ⋯ *or* 9) *Other information prohibited by the law or administrative regulations.*

It is easy to see that provisions like this are "vague, confusing and inconsistent" (Li, 2004). Yet similar provisions are present in many other internet regulations. Indeed, these provisions are so common that many Chinese seem to have "accepted" them. Few people attempted to challenge the legitimacy (or constitutionality) of such provisions. Obviously, such vague provisions can deter individual citizens from spreading "sensitive" information that may fall into one of the prohibited categories.

Internet Censorship and Its Resistance

This Part introduces some specific measures (or techniques) that China uses to control the internet. Although these measures in fact overlap with one another, for purpose of clarity, they are to be discussed separately here.

Blocking and Filtering Systems

The Chinese government consistently blocks the entire domain of certain websites that are hard to control, including some international news sources (i.e., BBC-Chinese), internal blogger servicer providers (i.e., facebook, blogger), and some other websites that often post criticism on China's human rights and social justice records (i.e., Amnesty International, Human Rights Watch, etc.) These websites are blocked regardless of their specific contents, partly because the ISPs of these websites are unlikely to "cooperate" with the Chinese government in censoring the internet content (ONI, 2005).

The general trend, though, seems to be that the Chinese government tries to filter specific "sensitive" contents rather than blocking the entire websites at the backbone level. For example, before the 2008 Olympic Games, the New York Times website was entirely blocked. During the Olympic Games, the site was partially "unblocked", rendering some URLs (Uniform Resource Locates) accessible while others inaccessible. Thus, the accessibility of a website does not guarantee that all the contents on that site will be available. Typically, the blocked contents are those that are deemed to be "sensitive" by the government. The specific "sensitive" contents change over time. However, certain contents are regularly filtered: for example, the Tiananmen Square protests of 1989, the independence of Tibet, Xinjiang and Taiwan, and the Falun Gong movement, etc. (Zittrain & Edelman, 2003; ONI, 2005).

With respect to filtering technology, China's technology is "the most sophisticated effort of its kind in the world". (ONI, 2005) As early as 1998, the Chinese government began to invest in the notorious Gold Shield software project. The main function of the Gold Shield software is to censor "illegal" contents. It can pick the sensitive words and block the relevant content. However, the effectiveness of filtering technology is unclear. The filtering systems can not foresee all the sensitive words. In addition, sophisticated internet users can often access blocked contents through various circumvention technologies.

Moreover, in recent years, as more and more individuals began to use internet, the resistance against such blocking and filtering practices also increases. The controversy over the "Green Dam Youth Escort" ("Green Dam" hereafter) provides a revealing example. The "Green Dam" software was a filtering device that was supposed to be very powerful in filtering internet contents. In May 2008, the Minister of Industry and Information (MII) spent more than 41 million yuan (about 6 million US dollars) to purchase the "Green Dam" software from two companies that had "cooperated" with Chinese government in the past. The MII then offered the software to internet users for free downloads. However, few individuals bothered to install the "free" software (Chao, 2009).

On May 19, 2009, the MII went further by sending a notification to computer manufacturers of its intention to require all new personal computers sold in China after July 1 to pre-install the "Green Dam" software. However, soon after the notification was released, there was a surge of online criticism. At the night of June 30, just several hours before the requirement was to become effective, MII issued a notice, declaring that the requirement to install the "Green Dam" software was to be postponed. Till day, the MII has not re-set the requirement for compulsory pre-installation of the software.

Controlling the ISPs and the Resulting Self-Censorship

As mentioned in Part 2, several regulations impose liabilities on ISPs, blog service providers (BSPs), and BBS (Bulletin Board System) providers, etc. For example, the 2000 Measures requires IAPs and ISPs to record the dates and times when subscribers accessed the Internet, the subscriber's account number, the addresses of all websites visited, and the telephone number used to access the Internet. The ISPs and IAPs must keep a record of this information for sixty days and provide it to the authorities upon request. Similar liabilities were imposed on BBS providers in another regulation promulgated in 2000.

Indeed, the Chinese authorities took specific actions to implement these regulations. For example, on January 9, 2009, Niubo, a blog service provider, was shut down because it transmitted "harmful information on political and current affairs" (Wu, 2009). Specifically, the closure was linked to its status as being the leading domestic circulator Charter 08, a proposal by Chinese intellectuals to reform China's politics (Garnaut, 2009).

Because of the threat of punishment, private entities (including IAPs, ISPs and BSPs) often resort to self-censorship. The following are some of the typical methods that are used by

these entities to "censor" the internet. First, like the government, the private entities also resort to the filtering technology. Some forum operators have developed their own systems to catch sensitive words so that they can review the message before it is posted. As a result, when an internet user attempts to post an entry which contains a "sensitive" word, he or she would receive an immediate notice stating "this message can not be posted because it contains improper content".

Second, these private entities also employ individuals to manually delete or conceal "sensitive" posts or comments. These individuals are commonly known as "internet administrators". Their routine job is to spot and delete (or conceal) posts or comments that are deemed to be "improper". To help these internet administrators identify "improper" or "sensitive" contents, many websites encourage individuals internet users to report such contents to the administrator by clicking certain icon.

Finally, if a blog or specific forum becomes too "sensitive", the ISP (or BSP) may delete or block the blog or forum. Thus, Sina.com, China's most popular BSP, shut down numerous blogs that are too "sensitive". Even some international corporations have yielded to the pressure. For example, in December 2005, Microsoft Corporation deleted the site of a Beijing blogger from its MSN Spaces service (Barboza & Zeller, 2006). This case drew much international attention partly because it involves Microsoft, a US-based corporation. It would not have gained much attention had it been a Chinese corporation.

Like government censorship, "private censorship" is increasingly being challenged by internet users. In recent years, there had been several well-known law suits in which the owner of the shut-down blogs sued the BSPs. For example, in August 2007, Liu Xiaoyuan, a lawyer in Beijing, sued Sohu.com for deleting his blog posts. He alleged that Sohu breached the blog service contract by concealing nine articles he posted on his blog. These articles, he alleged, were "neither illegal nor obscene." Although Lawyer Liu was able to file the lawsuit in a Beijing court, he soon received a court order stating that the court would not accept the case. Liu sought to appeal. But the appellate court refused to review the case (Tang, 2007).

While the plaintiffs in most of the cases, like Mr. Liu, were unable to get their cases filed in the court, Hu Xingdou turns out to be an exception. Mr. Hu is a professor at Beijing Technology University. He had a personal website on which he posted his own articles, most of which were political comments. He paid certain fees to Beijing Xinwang Corporation, a ISP which provided the technological support for his website. However, in March 2007, Mr. Hu received a notification from Xinwang, informing him that his website was shut down because it contained "illegal information". Mr. Hu then filed a suit in a Beijing court, alleging that Xinwang breached the blog service contract. More than twenty intellectuals in Beijing, including some prominent law professors and lawyers, signed a "public letter" to support Mr. Hu. Partly because of the media pressure, the court ruled in favor of Mr. Hu, stating that Xinwang did not provide any evidence regarding what was "illegal" on Mr. Hu's website.

Mr. Hu's victory was rather exceptional. According to Mr. Hu, he knew it would be impossible to win if he alleges that the ISP infringed his right to "freedom of speech". As a tactical choice, he only alleged that ISP breached the blog service contract. Also, he only asked for a refund of the fees, not the restoration of the website. As such, the court was able to render a decision without deciding whether Mr. Hu's free speech right has been abridged.

Access Control

Currently, Chinese internet users access the internet through three major channels: personal computers, mobile phones and internet cafes. The internet cafes are the main access location for about half of Chinese internet users (CINIC, 2009).

The Chinese government sought to control each of the three accesses. The first two accesses are relatively easy to control. An individual accessing the internet through a personal computer, whether at home or at office, can be easily located. Similarly, the mobile phone owners who accessed internet could be easily identified. The following part focuses on the Chinese government's attempts to control citizens' activities in internet cafes.

The government's control is implemented mainly through two layers of registration requirement. First, every internet cafe is required to register at a designated local governmental agency. Because local governments typically limit the number of the internet cafes in a particular locality, the registration process essentially involves governmental licensing. The government would only grants the license to internet cafes that meet certain requirements. The license may be revoked if the internet cafe does not follow the "rules". For example, between June and September 2002, the government shut down 150,000 unlicensed Internet cafes (Hermida, 2002). Till day, police routinely "raids" internet cafes to see whether there is any "illegal" activity going on.

The second layer of the access control occurs at the level of individual internet users. Internet cafes are required to record every user's identity and online activities. Each cafe is required to keep these records (or "logs") for at least sixty days and to provide the records to police upon request. Currently, these rules are strictly enforced. Thus, one who does not take his valid identification card with him may not access internet in internet cafes.

Finally, all cafes are required to install monitoring software approved by the police. Such software not only monitors online activities of internet users in the cafe, but also filters certain "sensitive" information.

Criminal and Administrative Punishment

A lot of individuals have been punished for "illegal" online activities such as posting prohibited contents. In 2008 alone, it was reported that China imprisoned at least forty-nine individuals for online activities, including several individuals serving their second period of detention for internet-related crimes (Reporters without Borders, 2009; China Human Rights Defenders, 2009). For example, Liu Shaokun, a school teacher, was sentenced to one year reeducation-through-labor for posting pictures of school buildings that collapsed in the 2008 Sichuan earthquake (Human Rights in China Press Release, 2008).

Individuals may even be punished for sending private e-mails that contain "sensitive" contents. For example, in 2005, Shi Tao, a Chinese citizen, was sentenced to ten years in prison for e-mailing a "state secret" to a New York website editor. The "top secret" reportedly expressed the Party's concern about the possibility of demonstrations occurring on the fifteenth anni-

versary of the Tiananmen Square protest. Shi used a Yahoo e-mail to send the information. The case drew international attention partly because Yahoo "cooperated" with the Chinese government by providing information linking the e-mail to the IP address of Shi's computer (Kerstetter, 2005).

In recent years, as the internet becomes to be used by more and more individuals, the resistance against government abuse is also growing. For example, in February 2009, Wang Shuai, while working in Shanghai, posted a blog entry stating that officials in his hometown, Lingbao City in Henan province, had misappropriated funds for combating drought. To the surprise of Mr. Wang, police from Lingbao arrested him in Shanghai. Fortunately for Mr. Wang, a report in China Youth Daily (a newspaper) sparked a heated online discussion. Finally, the media pressure became so great that the high Party officials in Henan province issued an apology, compensated Wang for his eight-day detention, fired the local Party secretary, and punished three officials who misappropriated funds (Chen, 2009).

Internet Police

In January 2006, the city of Shenzhen introduced two cartoon characters that appear on all websites or internet forums in Shenzhen. The cartoons move interactively with the internet users as they navigate through web pages. In addition to linking the users to information about internet regulations and internet-crime cases, the cartoons also connect users to internet police through an Instant Messaging service for the purpose of answering users' questions about internet security. However, as officials of Shenzhen Public Security Bureau informed the reporters, the "main function" of the cartoons is "to intimidate, not to answer questions" (Qiang, 2006).

The intimidation function seems to work. It was reported that between January and May 2006, the frequency of posting "hazardous information" decreased by sixty percent, and more than 1600 Internet crime allegations were reported through the cartoon police. Thereafter, the cartoon police were introduced in many other cities (Xinhua News Agency, 2006).

"Guiding" the Public Opinion

Partially in response to the uncontrollable nature of internet, the Chinese government attempted to "guide" public opinion by hiring "internet commentators." In 2008, a report estimated that China employed more than 280,000 "internet commentators" nationwide (Bandurski, 2008). While the government never explicitly spelled out the qualifications and functions of the "internet commentators", media reports suggest that they mainly perform two tasks: first, "guiding" the internet users towards "correct" political direction; second, identifying, and sometimes deleting "harmful" information.

The "internet commentators" originated at Nanjing university in 2005: the university recruited students with school funds to advocate the "correct" line on an online student forum. The practice soon became popular at different levels of government and other Party-controlled organizations. For example, Gansu province, a largely poverty-stricken province in Northwestern China, announced to recruit 650 "internet commentators" in 2009.

Besides, the Minister of Culture developed Internet commentator trainings. Those who went though the training would receive a job certification, which would qualify them to serve as "internet commentators". There seems to be plenty of job opportunities for these 'internet commentators": not only government hire "internet commentators", major websites are required to recruit in-house teams of the government-trained commentators.

Conclusion

While censoring the internet may have some beneficial effects from the government's perspective, it does more harm than good. There are at least four reasons to conclude that governments should not censor internet.

First, although censorship might keep "bad news" from being released to the public in the short run, it can rarely do so in the long run. In today's world, although censorship may make it more difficult for individuals to find certain "sensitive" information, it can not entirely block such information. For example, many individuals in China can actually use circumvention technology to access "sensitive" information.

Second, even assume that the government can "successfully" keep certain information from being transmitted to individual citizens, such a "success" is not necessarily good. Public decisions based on one-sided information are often problematic, and may sometimes lead to disastrous consequences.

Third, such censorship may destroy citizens' trust for the government. Individuals tend to suspect the news released by government. They may think that such news has been manipulated by the government. Such a situation could be devastating for the government in the long run.

Finally, the financial costs of such censorship are huge. The Chinese government has spent a lot of money on purchasing or developing the filtering software, hiring the "internet administrators" and "internet commentators", and implementing the censorship mechanism. It is hardly possible for a democratic government to spend so much money to curtail citizens' speech.

REFERENCES

Bandurski, D. (2008). China's guerrilla war for the web, far eastern economic review. URL (last checked 16 November 2012). http://www.feer.com/essays/2008/august/chinas-guerrilla-war-for-the-web

Barboza, D., & Zeller, T. (2006), Microsoft shuts blog's site after complaints in Beijing. *NY Times*. http://www.nytimes.com/2006/01/06/technology/06blog.html?_r=1&oref=slogin

Chao, L. (2009). China squeezes PC makers. *Wall Street Journal*. http://online.wsj.com/article/SB124440211524192081.html

Chen, J. (2009). Officials punished over land scandal. *Shanghai Daily*, 29 April 2009.

China Human Rights Defenders (2009). Tug of war over China's cyberspace: A sequel to journey to the heart of censorship. URL (last checked 9 March 2012). http://crdnet.org/Article/Class9/Class11/200903/20090319000543_14370.html

CINIC (China Internet Network Information Center) (2009). Twenty-third statistical survey report on the internet development in China. 23 March 2009.

Hermida, A. (2002). Behind China's internet red firewall URL (last checked 15 November 2012). http://news.bbc.co.uk/1/hi/technology/2234154.stm

Human Rights in China Press Release (2008). Family visits still denied to Sichuan school teacher punished after quake-zone visit. URL (last checked 29 July 2008). http://www.hrichina.org/public/contents/press?revision_Id=66556&item_Id=6652

Kerstetter, J. (2005). Group says Yahoo helped jail Chinese journalist. CNET NEWS.COM, 6 September 2005.

Li, C. (2004). Internet content control in China. *International Journal of Communications Law and Policy, 1*, 5

Newbold, J. R. (2003). Aiding the enemy: Imposing liability on US corporations for selling China internet tools to restrict human rights. University of Illinois Journal of Law, Technology & Policy.

Official Google Blog (2010). A new approach to China. URL (last checked 16 November 2012). http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

ONI (2005). Internet filtering in China in 2004-2005: A country study. URL (last checked 15 November 2012). http://opennet.net/sites/opennet.net/files/ONI_China_Country_Study.pdf

Qiang, X. (2006). Image of internet police: Jingjing and Chacha Online-Hong Yan. URL (last checked 17 November 2012). http://www.chinadigitaltimes.net/2006/01/image_of_internet_police_jingjing_and_chacha_online_hon.php

Reporters without Borders (2006). List of the 13 internet enemies. URL (last checked 16 November 2012). http://www.rsf.org/List-of-the-13-Internet-enemies.html

Reporters without Borders (2009). 2009 Annual report: China. URL (last checked 16 November 2012). http://www.rsf.org/enrapport57-China.html

State Council of China (2000). Measures for managing internet information services. URL (last checked 15 November 2012). http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/measures-for-managing-internet-information-services-2000.html.

Tang, X. (2007). Why delete my blog articles? Chongqing Fazhi Ribao, 29 October 2007. URL (last checked 15 November 2012). http://blog.sina.com.cn/s/blog_3eba51c501000b7l.html

Wu, V. (2009). Popular blog service provider shut down. *South China Morning Post*, 10 January 2009.

Xinhua News Agency (2006). Cyber police in Shenzhen to curb on-line crimes. 15 May 2006. URL (last checked 15 November 2012). http://news.xinhuanet.com/english/2006-05/15/content_4547731.htm

Zhao, Z. G. (2008). Development and administration of internet in China. URL (last checked 15 November 2012). http://www.china.org.cn/china/internetForum/2008-11/06/content_16719106.htm

Zittrain, J., & Edelman, B. (2003). Empirical analysis of internet filtering in China. URL (last checked 15 November 2012). http://cyber.law.harvard.edu/filtering/china/

