An Overview of Internet Regulation in China

Anne S.Y. CHEUNG and ZHAO Yun

Abstract: The content that is allowed on the Internet in China has always been strictly regulated; unsuitable content is organized under twelve general categories. As a result, guerrilla-style digital warfare is waged between the Chinese government and high-tech libertarians. The goal of Internet regulation for the authorities is to provide a "healthy" environment for both political and economic development.

By December 2012, the number of Internet users in China had reached 564 million, representing a drastic jump from just 620,000 users in 1997, when the China Internet Network Information Society (CNNIC) carried out its first survey (CNNIC 2013). It is not only "netizens" in China that have embraced the information revolution, but also the Chinese authorities. Yet what the Chinese Communist Party (CCP) desires is economic growth and prosperity, and increasing investment opportunities; it does not desire unfettered discussion that may disrupt social stability or threaten state security.

Content Regulation

Although freedom of expression is guaranteed under China's constitution, the CCP has been extremely cautious with any form of politically sensitive information, which is

often defined vaguely and broadly. The state authorities are armed with numerous pieces of legal regulation, backed by an elaborate system of control. Direct regulation by the state goes hand-in-hand with indirect methods of co-regulation with the Internet industry, which include detailed legal duties and liabilities on Internet service providers (ISPs) to filter illegal (or unwanted) information, monitor online activities, retain data, and report to the authorities.

The Great Firewall of China

The primary way of Internet control adopted by the Chinese government is through restricting access to cyberspace by marking a division between "global cyberspace" and "domestic cyberspace" using a virtual firewall, a massive filter, and a block system that are collectively known as the "Great Firewall." At the national level, only ten government-approved agencies are permitted to establish interconnecting Internet networks and to license the operation of ISPs. No individual or single unit is allowed to establish a direct international connection, as the primary entry and access points to China are under strict control. This structure arguably provides the basis for an "intranet," an internal network that can be shut off from the outside world, and for the creation of a firewall, which is a system of Internet blocks and filters to regulate access to politically undesirable and objectionable materials.

At various points in time, and depending on the region in China, sites blocked include Economist.com, Cable News Network, and the *New York Times*. YouTube, Facebook, and Twitter are also usually inaccessible in China, although this blockage is certainly not foolproof. Anti-blocking technologies (i.e., blocking the blockers) have been developed and used by netizens in China to bypass the censored system. A guerrilla-style digital warfare is constantly waged between the Chinese government and high-tech libertarians. The majority of average netizens in China, however, are living behind the so-called Great Firewall.

The Legal Rules Governing Unlawful Content

The content that is allowed on the Internet has always been strictly regulated in China. Under the Regulations on Internet Information Services of 2000, the production, duplication, release, and dissemination of content in nine categories are absolutely forbidden. This includes information that:

1. opposes the basic principles laid down in the Constitution;
2. endangers national security, discloses state secret, subverts the ruling regime, undermines national unity;
3. is detrimental to the honor and interests of the state;
4. instigates ethnic hatred or ethnic discrimination, or that undermines ethnic unity;

5. undermines the state's policy towards religions, or that preaches the teachings of evil cults or that promotes feudalistic and superstitious beliefs;
6. disseminates rumors, disturbs social order, or undermines social stability;
7. spreads pornography or other salacious materials; promotes gambling, violence, homicide, or terrorism; or instigates crimes;
8. insults or slanders other people, or infringes upon other people's legitimate rights and interests; or
9. contains other information prohibited by the law or administrative regulations.

In 2002, the Interim Provisions on the Administration of Internet Publication added one more forbidden area: that of "compromising public morality or the refined indigenous culture and traditions." Furthermore in 2005, the Provisions of the Administration of Internet News Information Services added two additional forbidden categories of information. They were "information inciting illegal assemblies, association, demonstrations, protest, and gatherings that disturb social order" and "information concerning activities of illegal civic associations." In total, therefore, under Chinese regulations there are twelve forbidden areas that should not be published or discussed on the Internet.

In addition, the scope of the aforesaid defined categories may expand. In 2013, the Supreme People's Court and the Supreme People's Procuratorate issued a joint

Interpretation Concerning Several Issues of the Application of Law in Handling Criminal Cases in the Use of Information Networks Governing Criminal Defamation and other Crimes (hereinafter referred as Joint Judicial Interpretation). Information networks are defined to include the Internet, television broadcasting, fixed-line telephones system and mobile devices information system. Under the Joint Judicial Interpretation, criminal defamation under article 246 of the Criminal Law will now include e the "intentional fabrication" and dissemination of false information in information networks that "seriously endanger social order and national interest." Under the Criminal Law, fabrication of false information about others under "grave circumstances" may lead to a maximum of three years' imprisonment, criminal detention, surveillance or loss of political rights. Furthermore, under the 2013 Joint Judicial Interpretation "grave circumstances" cover information in the information networks that has been visited more than 5000 times or reposted by others for more than 500 times; or result in the injured party or his close relatives suffering from mental disorder, committing self-harm or suicide, or other serious consequence; or the defaming party has already been subject to administrative punishment for defamation in the preceding two years; or any other serious consequences. Another critical provision in the Criminal Law provides that criminal defamation may be brought by aggrieved parties, and by agents of the state in cases "where serious harm is done to

public order or to the interests of the state." According to the Joint Judicial Interpretation, the latter includes defamation in the information networks that cause (1) a mass incident; (2) public chaos; (3) ethnic or religious conflicts; (4) defamation of multiple persons that creates a repugnant social impact; (5) harms the national image or seriously endanger national interest; (6) causes a repugnant international impact; or (7) other situations that may gravely endanger social order and national interests. Hence, the offences under the Joint Judicial Interpretation are vaguely defined in both their conceptual definitions, their scope and punishment. It has been criticized of its chilling effect on Internet free speech (Lubman).

In fact, netizens in China always have to navigate carefully through the legal minefield. A notorious example of one who failed to do so is Liu Xiaobo, the Nobel Peace Prize Winner of 2010. In 2009, he was sentenced by the Chinese authorities to eleven years in prison for "inciting to overthrow state power" for co-drafting and posting a manifesto, "Charter 08," on the Internet. The manifesto called for political reforms, the end of corruption, and respect for human rights.

As is discussed in the following section , state agencies are not only required to carry out direct regulation on Internet content through various means, but the Internet industry is also given the duty of co-regulation.

Direct Regulation

Under the law, every individual, organization, and company in China is held criminally liable for sending harmful content as defined by law. Other than legal measures, the government has also attempted to control and "purify" Internet content through technological means. For example, in 2009, the government attempted to require the installation of Green Dam Youth Escort software to restrict access to "unhealthy" websites for all computers sold in China. This was done in the name of screening out pornographic materials and to protect the youth. Eventually, the project was abandoned due to a large public outcry from netizens in China, and from the international business community.

In addition to using legal means and technological advances to control the Internet, it is believed that in 2004, the CCP already had a special task force of more than 30,000 cyber police to patrol the Internet, to block foreign news sites, and to terminate domestic sites with politically sensitive information (Watts 2005). Starting also in 2004, different provinces in China recruited members of the so-called 50 Cent Party: undercover Internet commentator, who actively contribute pro-government statements on the Internet in chat rooms and on forums. (The term "50 Cent Party" reflects the amount that an undercover commentator would be paid for each

posting—which is actually about 8 cents.) In this way, public opinion is being shaped by the authorities.

Co-Regulation

Other than imposing direct control on users, the Chinese authorities have built a co-regulatory regime, imposing various duties and liabilities of filtering, monitoring, and reporting on the Internet industry.

Internet service and content providers are regulated directly under the Regulation on Internet Information Services of 2000. The general rule is that all Internet service providers are required to provide online users with quality services and to ensure the "legality" of the information. ISPs that offer news coverage and bulletin board services are required to keep a 60-day record of the information that they distribute, when it is distributed, and the web address where the information is located. Other ISPs are similarly required to keep records of the time of use, accounts of Internet addresses or domain names, and dial-in telephone numbers of online users for 60 days. The measures are considered the prime model for the strict control of Internet administration. In addition, the Law on Guarding State Secrets amended in 2010 imposes a duty on ISPs to keep records on the disclosure of information involving state secrets, and to report to state organs.

Electronic bulletin service providers, including those that disseminate information through online interactive forums, electronic bulletin boards, electronic white boards, Internet forums, online chat rooms, and message boards are governed under the Electronic Bulletin Services Provisions of 2000. They are also required to keep a record of users, monitor their activities, and report any violations to the authorities. Similar duties of data retention and reporting to the authorities extend to Internet email service providers under the Measures for the Administration of Internet Email Services of 2006. In addition to the duties of keeping record, monitoring, and reporting, Internet news information service providers, including websites, are required to reproduce content from official news organizations under the Provisions for the Administration of Internet News Information Services (2005).

Draconian as it may sound, regulation, co-regulation, and self-regulation became the prevailing style of rule after 2000. Other than keeping records and reporting unlawful content or behaviors, Internet cafés, Internet bars, computer lounges, and other places that provide Internet access to the public are required to install tracking software, institute surveillance and monitoring measures, and report to the relevant authorities if a user employs the Internet for illegal activities (article 19 of the Regulations on the Administration of Business Sites of Internet Access 2002). In addition to this structure, Internet publishers, web portals, and web managers are also

required to shoulder monitoring duties under the Interim Provisions on the Administration of Internet Publication of 2002. In March 2005, the Registration Administration Measures for Non-Commercial Internet Information Services stipulates that all owners of personal websites and webmasters of bulletin boards and blogs must register with the government, with violators risking a heavy fine or closure of their web pages.

The same standard also applies to providers of Internet cultural products, which are defined under article 2 of the Interim Provisions on the Administration of Internet Culture (issued in 2003, amended in 2011) to be Internet entities that produce, disseminate, or circulate audio and video products or game products; or show plays, works of art, cartoons, or other cultural products. ISPs and other intermediaries are part of the co-regulatory team of Internet control in China. In early 2011, *Time* reported that Sina Weibo (a large microblogging service) employed up to 700 censors to track and block content (Ramzy 2011). Companies (including Microsoft's MSN and Yahoo!) have generated their "block-lists" based on educated guesswork, which easily results in over-blocking of content (MacKinnon 2009).

The role of the ISP is illustrated in the 2004 Shi Tao case, where Yahoo! turned over information about the Chinese journalist Shi Tao to the Chinese authorities. Little did Shi know that the anonymous email he sent to a human rights organization in the

United States through his Yahoo! account would get him a ten–year prison sentence. He was convicted for illegally providing state secrets outside the country. In the foreseeable future, ISPs are likely to assume an increasing active and compliant role in reporting any suspects under the real name registration system when everyone who uses information services (including Internet and phones) have to register with their real names and identity numbers starting from September 2013 under the Provisions on the Registration of Real Identity of Telephone Users by the Ministry of Industry and Information Technology, and the Decision Concerning Strengthening Network Information Protection by the State Council.

Intellectual Property Rights

Rapid development of information technology poses serious challenges to the traditional legal regime for intellectual property rights. China has been able to quickly come up with legislation for intellectual property protection in this information era. Important developments have taken place in the following two major areas: protection of computer software, and domain name disputes.

Protection of Computer Software

The first regulation relating to the protection of computer software was made in 1991. A dual-track system was created for domestic and foreign software; namely, there is no registration requirement for foreign software and the protection period is fifty

years, while registration is required for domestic software and the protection period is twenty-five years, with the possibility of extension for another twenty-five years. Such discriminatory practice did not last long. In 1993, the Supreme People's Court abolished the requirement of registration, but the different protection periods still existed.

The situation changed completely when the new Regulations on the Protection of Computer Software was enacted in 2001 by the State Council. Registration is not compulsory under the newer regulation, but the registration certificate can serve as preliminary proof of ownership.

Software is normally owned by the author (i.e., creator) who develops it. When it comes to joint authorship, the ownership is determined by the written agreement among the authors. The software copyright owners enjoy the rights of publication, authorship, revision, duplication, lease, and translation. Economic rights are protected for the lifespan plus fifty years if the copyright owner is an individual, or fifty years after first publication for corporations who own copyrights.

The user is not allowed to reproduce, publish, or distribute the software without the consent of the owner. Copyright infringements include situations where the user intentionally avoids or breaches the technical measures adopted by the owner

to protect the software copyright, or intentionally deletes or alters the electronic information of software right management.

Domain Name Disputes

The CNNIC was set up as a non-profit organization in 1997. One major function of the CNNIC is to serve as a domain name (.cn) registry and manager. In view of the rapid development of domain name dispute resolution around the world, the CNNIC adopted the Chinese Domain Name Dispute Resolution Measures in 2000, which was later revised in 2002, 2006 and 2012.

The Chinese Domain Name Dispute Resolution Measures intends to use an alternative dispute resolution procedure to resolve domain name disputes in a quick, cheap, and fair manner. To win the case, the complainant needs to prove the following three elements: 1) the disputed domain name is identical or confusingly similar to the name or mark in which the complainant has civil rights and interests; 2) the disputed domain name holder has no lawful rights or interests in respect to the domain name or the major part of the domain name; and 3) the disputed domain name holder has registered or has used the domain name in bad faith.

Emerging Problems

Other than minding the political and economic dimensions of Internet governance, the authorities have to tackle the problem of privacy violations when netizens use the

Internet as a "human flesh search engine" (*rénròu sōusuǒ* 人肉搜索), a somewhat alarming-sounding name for collaboration by many people who use the Internet to expose the personal information and privacy of wrongdoers as a form of social punishment. (The term "human flesh" refers to the fact that these online searches lead to real people, and thus have real consequences.) Though some may applaud this as an alternative means to check against officials' abuse of power, the result can be devastating to ordinary citizens. Victims face various forms of harassment, people lose their jobs, and at least one has lost her life. In 2010, the new Tort Law became effective, with provisions to protect citizens' right of privacy, name, and reputation. Yet the phenomenon of human flesh search hunting has not stopped. An effective and comprehensive piece of legislation on personal information protection is yet to be enacted, which is essential for e-banking, electronic medical records, and other aspects of privacy protection on the Internet frontier.

Anne S. Y. CHEUNG & ZHAO Yun

The University of Hong Kong

Further Reading

Bandurski, David. (2008). China's guerrilla war for the web. *Far Eastern Economic Review, 171*(6) Jul/Aug, 41–44.

Cheung, Anne S. Y. (2006). The business of governance: China's legislation on content regulation in cyberspace. *New York University Journal of International Law and Politics*, 38(1–2), 1–37.

China Internet Network Information Centre (GIFC). (2011). The statistical reports of Internet development in China. Retrieved September 22, 2013, from http://www1.cnnic.cn/en/index/0O/index.htm

Diebert, Ronald; Palfrey, John; Rohozinski; Rafal; & Zittrain, Jonathan. (2008). *Access denied*. Cambridge, MA: The MIT Press.

Gao Fuping. (2004). The E-commerce legal environment in China: Status quo and issues. *Temple International & Comparative Law Journal*, *18*, 51–75.

Global Internet Freedom Consortium. (2007). Defeat Internet censorship: Overview of advanced technologies and products. Retrieved September 22, 2013, from http://www.internetfreedom.org/archive/Defeat_Internet_Censorship_White_Paper.pdf, 1-22.

Lubman, Stanley. (2013). The 'Legalization' of China's Internet Crackdown. *Wall Street Journal Blog.* September 18, 2013. Retrieved September 22, 2013, from http://blogs.wsj.com/chinarealtime/2013/09/18/the-legalization-of-chinas-internet-crackdown/

MacKinnon, Rebecca. (2009). China's censorship 2.0: How companies censor bloggers. *First Monday*, *14*(2). Retrieved September 22, 2013, from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089.

Miao, Felix. (2007–2008). Protection of intellectual property rights in software products and how to accomplish a technology transfer transaction in China. *Fordham Intellectual Property, Media & Entertainment Law Journal*, 18, 61–115.

Ramzy, Austin. (2011). Wired up. *Time,* 21 February 2011. Retrieved September 22, 2013, 2011, from http://www.time.com

Watts, Jonathan. (2005). China's secret Internet police target critics with web of propaganda. *Guardian,* 14 June 2005. Retrieved September 22, 2013, from http://www.theguardian.com/technology/2005/jun/14/newmedia.china

Zhang Chu; & Lei Lingfei. (2005). The Chinese approach to electronic transactions legislation. *Computer Law Review & Technology Journal*, 9, 333–354.

Zhang Mo. (2002). Governance of Internet Domain Names against Cybersquatters in China: A Framework and Legal Perspective, *Hastings International & Comparative Law Review*, 26, 51–81.

Zhao Yun. (2009). Reflection on the Finality of Panel's Decisions in Domain Name Dispute Resolution Process, with Reference to China's Practice, *John Marshall Journal of Computer & Information Law*, 26, 395-413.

Zheng Yongnian. (2008). Technological Empowerment: The Internet, State, and Society in China. US: Stanford University Press.

Zittran, Jonathan & Edelman, Benjamin. (March 20, 2003). *Empirical Analysis of Internet Filtering in China*, Retrieved September 22, 2013, from http://cyber.law.harvard.edu/filtering/china/.