CHN101060.E

China: Internet censorship, including state regulations, technical control, enforcement, and methods used to avoid censorship (2005 - 2006)
Research Directorate, Immigration and Refugee Board of Canada, Ottawa

General information

In its most recent report, the state-run organization China Internet Network Information Center revealed that there were 103 million Internet users in China in 2005 (CNNIC July 2005; CNNIC n.d.). Human Rights Watch (HRW) estimated that the number of Internet users in China had reached 111 million, or 8 per cent of the population, by the end of 2005 (HRW 2 Feb. 2006; see also Globe and Mail 21 Feb. 2006). Use of the Internet, according to The Guardian, was "spreading beyond [the] well-regarded middle class and into the more disgruntled factory and farming communities" (14 June 2005), and is expected to increase as the country experiences rapid economic growth and the Chinese government encourages the development of the Internet (US 22 Nov. 2005, 2). In June 2004, Reporters Without Borders (RSF) stated that the number of Websites approved by the authorities in China had increased by 60 per cent from 2002, and that Internet businesses, such as portals, were "booming" (RSF 22 June 2004).

Censorship of the Internet

In a study of Internet filtering in China, the OpenNet Initiative, a partnership between the Citizen Lab at the University of Toronto, the Berkman Center for Internet & Society at Harvard University, and the Advanced Network Research Group at the University of Cambridge, commented that China employed the "most sophisticated" program of Internet censorship in the world (OpenNet Initiative 14 Apr. 2005, 3). Through a combination of technical control and legal regulation, and with the participation of numerous governmental organizations and private personnel, the Chinese government censored different types of Internet content, including Web pages, online discussion forums, online diaries known as Web logs (or "blogs"), e-mail messages and university bulletin board systems (ibid.). According to RSF, the government also utilized "a clever mix of propaganda [and] disinformation" and promoted self-censorship, since "complete control of electronic communication is impossible" (RSF 22 June 2004). The OpenNet Initiative study found the filtering system to be complex and in continual flux, and thus difficult to describe "with precision" (14 Apr. 2005, 3).

Topics identified by government authorities as being "sensitive" and subject to censorship include Tibetan and Taiwanese independence, the Falun Gong, the Tiananmen Square incident, anti-Communist Party movements and opposition political parties (OpenNet Initiative 14 Apr. 2005, 3). When, in June 2005, Microsoft agreed to censor messages on its Web log service in China, key words targeted included "freedom," "democracy," "demonstration," "human rights," and "Taiwanese independence" (BBC 14 June 2005), along with "Dalai Lama," and "China + corruption" (RSF 15 June 2005). According to The Guardian newspaper, the Chinese government is interested in eliminating any material on the Internet that could encourage organized opposition to the regime (26 Jan. 2006). The state news agency Xinhua, however, described censorship of the Internet as being aimed at curbing "superstitious, pornographic, violence-related, gambling and other harmful
information" (Xinhua 7 Oct. 2005). Websites that have been blocked in China include the British Broadcasting Corporation (BBC), Voice of America (US 22 Nov. 2005, 3; ibid. 3 June 2004), Wikipedia, an online encyclopaedia (US 22 Nov. 2005, 3; Courrier international 15 Feb. 2006), Google’s cache - which provides "snapshots" of pages of Websites otherwise blocked - the search engine Alta Vista, and the Websites of a number of human rights organizations, including Amnesty International (AI), Human Rights Watch (HRW), Human Rights in China, Reporters Without Borders (RSF), and China Labor Bulletin (US 3 June 2004).

State Regulations and Policies

According to the OpenNet Initiative, the legal apparatus regulating the Internet in China is complex, involving at least a dozen governmental organizations with responsibility for Internet access and content, in keeping with expanding and often overlapping regulations (14 Apr. 2005, 8). Regulations dating from 2000 outline registration procedures for Websites and annual inspections of Internet businesses (OpenNet Initiative 14 Apr. 2005, 9). Internet Service Providers (ISPs) are required by law to obtain a license from the Ministry of Information Industry (MII), and to keep records of their clients' account numbers, time spent online and sites visited (ibid. 9, 11). This information must be kept for 60 days and given to government authorities upon request (ibid., 11; see also US 3 June 2004). Users who take out a subscription with an ISP must register with the local public security bureau within 30 days (OpenNet Initiative, 10). For their part, Internet Content Providers (ICPs) that offer online news or operate bulletin boards must monitor all content and remove from their Web pages any postings that contravene the law (ibid., 10). ICPs are also required to record subscribers' usage for up to 60 days and provide the information to the government upon request (ibid., 10; see also US 3 June 2004).

Internet users are bound to prohibitions under 1997 regulations issued by the Ministry of Public Security, including using the Internet to "harm national security; disclose state secrets; harm the interests of the State, of society, or of a group; or to take part in criminal activities" (OpenNet Initiative 14 Apr. 2005, 13). The regulations also prohibit the use of the Internet to resist the country's laws, to threaten national unity and social order, to promote superstitions and sexually suggestive material, and to harm computer information networks (ibid.). Violating these regulations could lead to fines and termination of Internet access for up to six months (ibid., 13-14). The Law of the People's Republic of China on Guarding State Secrets is, according to the OpenNet Initiative, a "critical and broadly defined part of China's Internet content control" program (ibid., 16). The Law breaks down the definition of state secrets into various categories, such as restricted information related to national defence, policy decisions, political parties, and scientific and technological development (ibid.). It also gives the State Secrets Bureau an extensive role in deciding what constitutes a state secret, and stipulates that citizens may receive the death penalty if they are found to have used the Internet to provide state secrets to foreigners (ibid.). The BBC reported that owners of "blogs" (Web logs) in China were required to register with authorities by 30 June 2005 or face criminal charges (10 June 2005). A well-known blogger who spoke to Asia Times Online, however, reported that requirements associated with registering a blog, such as removing links to sites not approved by the government and the registration fee of 500 yuan (US$60), were difficult to meet (Asia Times Online 15 June 2005). A Web-based crawler program was also being installed to monitor content of Web logs and report any unregistered sites (BBC 14 June 2005). There were reportedly 700,000 Web logs in operation in China, while access to non-Chinese-based Web logs was prohibited (BBC 10 June 2005).

Cyber cafés are subject to regulations that require them to install software that blocks access to questionable content, including pornographic material, to keep detailed records of Web pages viewed by their customers, and to turn these records over to the Public Security Bureau (OpenNet Initiative 14 Apr. 2005, 11-12; see also BBC 14 Feb. 2005). Internet cafés must be licensed to operate - although a number of active cafés are not (OpenNet Initiative 14 Apr. 2005, 11, 12) - and are subject to strict opening hours and are open only to patrons 16 years of age and older (ibid.; see also BBC 14 Feb. 2005). There are reportedly about 100,000 cyber cafés in China, frequented by a significant proportion of Internet users who cannot afford personal computers (ibid.). Cyber cafés are monitored by government authorities on a regular basis (OpenNet Initiative 14 Apr. 2005, 11).

On 25 September 2005, new regulations governing news content on the Internet were introduced (BBC 26 Sept. 2005; HRW 28 Sept. 2005; US 22 Nov. 2005, 4-5; China Daily 26 Sept. 2005). The regulations, which update rules dating from 2000, restrict the distribution and publication on the Internet of news that has not been officially censored, thus requiring Internet portals to publish only news and commentary directly from official sources (HRW 28 Sept. 2005). The new regulations also prohibit content that promotes superstitious beliefs, spreads rumours, threatens national unity or encourages gatherings disturbing social order (ibid.). HRW points out that terms like "national security" and "social order" have been "left purposefully undefined in the interests of putting an end to words or activities that might challenge one-Party control" (28 Sept. 2005).
Under the new regulations, private individuals and groups must register as a "news organization" in order to operate Websites or e-mail distribution lists for news dissemination (US 22 Nov. 2005, 5), a requirement that HRW states "ensures that only groups that parrot the government's version of events will have e-mail distribution privileges" (HRW 28 Sept. 2005). Operators of Websites that violate these regulations may face fines and threats of closure (US 22 Nov. 2005, 5). Online bulletin boards and cellular phone text messages are also subject to the new regulations (ibid.; BBC 26 Sept. 2005; HRW 28 Sept. 2005; China Daily 26 Sept. 2005). Information on the enforcement of the new regulations could not be found among the sources consulted by the Research Directorate.

In February 2006, Xinhua News Agency reported that the Chinese government would soon introduce a regulation prohibiting e-mails for advertising purposes sent without the receiver's permission (globeandmail.com 21 Feb. 2006). All unsolicited e-mail advertisements would also be required to carry a subject line entitled "advertisement" (ibid.). Details about penalties and when the new regulation would go into force, however, were not available (ibid.).

Technical Controls

According to Reporters Without Borders (RSF), "[t]he architecture of the Chinese Internet was designed from the outset to allow information control [as it has] just five backbones or hubs through which all traffic must pass" (RSF 22 June 2004). The OpenNet Initiative concluded from its study that filtering of Internet content occurs "primarily at the backbone level of China's network" (14 Apr. 2005, 3), that is, on the router system (US 22 Nov. 2005, 5). The routers ensure that Uniform Resource Locators (URLs), or the Internet addresses of files located on a computer (State University of New York 9 May 2005), travel through proxy servers which scan for "politically sensitive words" in the URLs (US 22 Nov. 2005, 5-6). When such a word is identified, the router will send an error message to the Internet user, such as "file not found" (ibid., 6; see also OpenNet Initiative 17 Apr. 2005, 21-22). It is also reportedly possible that a person attempting to access a blocked site would be redirected to a different site or to an invalid Internet address, causing the user to believe that he or she has the wrong address (RSF 22 June 2004). The findings of the OpenNet Initiative indicate that blocking of sensitive Internet content such as Falun Gong or Taiwan, while not perfect, is "extensive," and sometimes results in "overblocking," meaning that "sites with superficial similarities to those with sensitive material, but different content, were filtered" as well (OpenNet Initiative 17 Apr. 2005, 23).

E-mail filtering, according to the OpenNet Initiative study, does not appear to take place on the router, or backbone, system but is rather undertaken by e-mail service providers (ibid., 46). Results of tests conducted by the OpenNet Initiative reveal that there is little consistency in e-mail filtering among service providers (ibid., 47). For example, testers were able to successfully send messages in English on topics related to religious freedom and media censorship to e-mail accounts with Chinese e-mail service providers, but had less success with similar messages in Chinese (ibid., 46-47).

Chinese search engines also perform Internet content filtering (ibid., 49). Through a series of tests, the OpenNet Initiative confirmed claims by RSF that Baidu.com and Yisou.com filtered search queries by keyword and removed certain sites from the results page (ibid., 49). However, filtering of Internet searches occurs on the router system as well (ibid.). In January 2006, the search engine Google launched its Chinese-language service, announcing that it would restrict certain search terms and would alert the user when results had been removed from the page (The Economist 26 Jan. 2006; see also BBC 25 Jan. 2006). The BBC reported that, after entering a query on the Falun Gong on Google.cn, it was redirected to a set of articles condemning the spiritual movement (ibid.).

Chinese online discussion forums, which RSF stated in 2003 were used by tens of thousands of Internet users, are equipped with filtering systems to sort out messages containing banned words (RSF 12 May 2003). Discussion forum moderators are also responsible for removing comments that do not conform to rules regarding acceptable content (ibid.). In tests conducted by RSF, the organization found that discussion forums applied this system of censorship with varying degrees of strictness (ibid.). Discussion forums found on state-sponsored news Websites such as xinhuanet.com contained no critical comments, while forums operated by commercial enterprises appeared to be more open and willing to "test the limits of censorship" (ibid.). Overall, RSF found that 30 per cent of messages containing "controversial content" - for example, a call for free elections and the release of human rights activists - that it had tried to post on Chinese discussion forums were accepted (ibid.).

Enforcement of Internet Censorship Rules

The Ministry of Public Security (MPS) has responsibility for the overall regulation of Internet access
Internet users can evade the filtering system by using proxy servers rather than the government-controlled network to go online (BBC 10 Mar. 2004; The Guardian 26 Jan. 2006; The New York Times 29 Jan. 2006). Volunteers at computers located outside of China act as an intermediary for requests to access the Internet from within China and provide access to blocked Websites by changing their URLs (ibid.; BBC 10 Mar. 2004). One software program that allows users in China to access servers abroad is Freagate, developed by expatriate Chinese volunteers in the United States (The Wall Street Journal 13 Feb. 2006; see also BBC 10 Mar. 2004) and financed by the US government and the non-profit organization Human Rights in China, among others (The Wall Street Journal 13 Feb. 2006). According to its inventor, on a daily basis, about 100,000 Internet users in China use Freagate or one of two similar programs his company has produced (ibid.). Voice of America and Radio Free Asia, whose Websites are blocked by the Chinese filtering system, employ the company to send e-mails to China featuring links to their news items (ibid.).

Since information about circumventing filtering controls sent via e-mail can potentially be viewed by police monitors, the Citizen Lab at the University of Toronto is devising a program called Psiphon that would allow volunteers outside China and Chinese Internet users to exchange encrypted information about circumvention in a secure manner (BBC 10 Mar. 2004; The Globe and Mail 13 Feb. 2006). In addition to Citizen Lab, a number of other organizations, such as the Electronic Frontier Foundation, Peacefire.org and Dynamic Internet Technology, are devising ways to allow Chinese Internet users to circumvent filtering controls (The
New York Times 29 Jan. 2006). According to a media company specializing in the Chinese market, authorities appear to be unable to prevent Web log entries made via proxy servers (The Guardian 26 Jan. 2006). Only a small number of Internet users in China, however, made use of software programs such as Freegate, a Web log user told The Wall Street Journal, adding that most Chinese "have not realized the harmful effects from network blocking!" (The Wall Street Journal 13 Feb. 2006). As one independent Internet researcher remarked to the BBC, the majority of Chinese Internet users were not interested in being "cyber dissidents," and it remained unclear what proportion of Internet users in China were looking to circumvent Internet content controls (BBC 10 Mar. 2004).

This Response was prepared after researching publicly accessible information currently available to the Research Directorate within time constraints. This Response is not, and does not purport to be, conclusive as to the merit of any particular claim for refugee protection. Please find below the list of additional sources consulted in researching this Information Request.

References


Additional Sources Consulted

Internet sites, including: Citizen Lab, Xinhua News Agency.

The attached reproduction is a copy of an official work that is published by the Government of Canada. The reproduction has not been produced in affiliation with, or with the endorsement of the Government of Canada.