

1630 Connecticut Avenue, NW Suite 500
Washington, DC 20009
Telephone: 202-612-4321
Facsimile: 202-612-4333
Email: hrwdc@hrw.org
Website: <http://www.hrw.org>

FREEDOM OF EXPRESSION AND THE INTERNET IN CHINA: A Human Rights Watch Backgrounder

INTERNET IN CHINA

As the Internet industry continues to expand in China, the government continues to tighten controls on on-line expression. As recently as July 11, 2001, President Jiang Zemin condemned the spread of “pernicious information” on the Net and called existing legislation “inadequate.”¹ Since 1995, when Chinese authorities began permitting commercial Internet accounts, at least sixty sets of regulations have been issued aimed at controlling Internet content. The broadly-worded regulations represent a clear violation of the right to freedom of expression, and the government is devoting considerable time and resources to trying to implement them.²

As of January 2001, sending “secret” or “reactionary” materials over the Internet became a capital crime. Generally, however, persons convicted for their use of the Internet have received sentences of between two and four years, and we are not aware of anyone having been charged under Internet-specific regulations. Instead, they have all been found guilty of violating provisions of the Criminal Code. The elaborate regulatory framework serves, however, as a statement of policy, a justification for monitoring and surveillance, a set of guidelines for what constitutes “illegal” activity, and a deterrent to Internet users.

The government’s determination to censor on-line content has grown with Internet usage. Improved infrastructure, introduction of mobile phones, and other low-cost methods of connection to the Internet, as well as increased local language content, have fueled that growth. The main contact points connecting China’s Internet system with the worldwide system consists of nine so-called Internet Access Providers controlling the physical lines to the outside world. By July 2001 these access providers accommodated some 620 Internet Service Providers (ISPs) who served in turn some 1,600 Internet Content Providers (ICPs) and an estimated 26,000,000 users by the government’s own conservative estimates.³

This backgrounder examines the development of China’s repressive regulatory framework, its surveillance and closures of Internet cafés, and the detention of Internet users.

RULES AND REGULATIONS

Between 1994 and the present, China's rules and regulations on the Internet became progressively more comprehensive, moving from efforts to regulate Internet business to restrictions on news sites and chat rooms. These regulations give the government wide discretion to arrest and punish any form of expression. For example, "topics that damage the reputation of the State" are banned, but an Internet user has no way of knowing what topics might be considered injurious. As the regulatory framework evolved, the Chinese government shifted primary responsibility for control of the Internet from the Ministry for Public Security to the Internet service providers themselves.

In 1994, one year before the Internet became commercially available for individuals in China, the State Council issued the "PRC Regulations for the Safety Protection of Computer Information Systems"⁴ which gave the Ministry of Public Security overall responsibility for supervision of the Internet. According to Article 17 of the Regulations, Public Security is entitled to "supervise, inspect and guide the security protection work," "investigate and prosecute illegal criminal cases" and "perform other supervising duties." In February 1996, the State Council issued rules on the connection between China's domestic network and the international Internet.⁵ These regulations began to shift some of the responsibility for control of content to the Internet companies themselves. Article 11 of that order reads:

Units providing international inward and outward channels and interactive and interfacing units shall establish a network management center to strengthen the management of their own units and their consumers according to the relevant laws and state regulation, to improve network information security management, and to provide good and safe services to consumers.

Article 13 continues:

[U]nits and individuals engaging in Internet business shall strictly enforce safety and security control systems according to relevant state laws and administrative regulations, and shall not make use of the Internet to conduct criminal activities – including activities prejudicial to state security and the leakage of state secrets – or to produce, retrieve, duplicate, and disseminate information prejudicial to public order or pornographic materials."

Public Security then issued a decree that all Internet users register with a police bureau in their neighborhood within thirty days of signing up with an ISP. Police stations in provinces and cities followed up on this almost immediately. They also set up computer investigation units. In December 1997, Article 5 of the "Computer Information Network and Internet Security, Protection and Management Regulations," issued by the Ministry of Public Security, states:

No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information:

1. Inciting to resist or violate the Constitution or laws or the implementation of administrative regulations;
 2. Inciting to overthrow the government or the socialist system;
 3. Inciting division of the country, harming national unification;
 4. Inciting hatred or discrimination among nationalities or harming the unity of the nationalities;
 5. Making falsehoods or distorting the truth, spreading rumors, destroying the order of society;
 6. Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder,
 7. Engaging in terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people;
 8. Injuring the reputation of state organs ;
- Other activities against the Constitution, laws or administrative regulations.

Article 8 of the same regulations states:

Units and individuals engaged in Internet business must accept the security supervision, inspection, and guidance of the Public Security organization. This includes providing to the Public Security organization information, materials and digital document, and assisting the Public Security organization to discover and properly handle incidents involving law violations and criminal activities related to computer information networks.⁶

The main two sets of regulations that foreign investors such as AOL will have to confront are the “Telecommunications Regulations Of The People's Republic Of China” and the “Measures For Managing The Internet Information Services,” both issued by the State Council and effective from September 25, 2000.⁷

Article 57 of the Telecommunications Regulations state that

No organization or individual may use telecommunications networks to make, duplicate, issue, or disseminate information containing the following:

- (1) Material that opposes the basic principles established by the constitution;
- (2) Material that jeopardizes national security, reveals state secrets, subverts state power, or undermines national unity;
- (3) Material that harms the prosperity and interests of the state;
- (4) Material that arouses ethnic animosities, ethnic discrimination, or undermines ethnic solidarity;
- (5) Material that undermines state religious policies, or promotes cults and feudal superstitions;

- (6) Material that spreads rumors, disturbs social order, or undermines social stability;
- (7) Material that spreads obscenities, pornography, gambling, violence, murder, terror, or instigates crime;
- (8) Material that insults or slanders others or violates the legal rights and interests of others;
- (9) Material that has other contents prohibited by laws or administrative regulations.

Meanwhile the “Measures For Managing The Internet Information Services” make service providers responsible for content they display. Articles 14 through 16 of these regulations could easily be used to curb freedom of expression. Article 14 says that the service providers must record their subscribers’ access to the Internet, their account numbers, the Web addresses they call up as well as the telephone numbers they use, and store this information for sixty days. Article 15 repeats the eight categories of information that is not to be produced on the Internet. Article 16 then goes on saying that if material under these categories is discovered, "it shall immediately stop the transmission, keep the relevant records, and report the situation to the relevant state authorities."

Other regulations that content providers have to face include the “State Secrets Protection Regulations For Computer Information Systems On The Internet” issued by the Bureau for the Protection of State Secrets (State Secrets Bureau) on January 25, but applied retroactively from January 1, 2000.⁸

Article 8 of this ruling states:

The management of secrets concerning information on the Internet shall be based on the principle of "whoever places materials on the Internet takes the responsibility." Information provided to or released on Web sites must undergo a security inspection and approval. Inspection and approval should be carried out by related departments. Related units shall, in line with state laws and regulations on guarding secrets, establish and improve a leadership responsibility system for the examination and approval of information intended for the Internet. Units that provide the information shall establish a security system for information examination and approval in accordance with certain work procedures.

Article 10 of the State Secrets Regulations states:

Units and users that establish electronic bulletin boards, chat rooms or network news groups shall be verified and approved by the relevant organizations to clarify the requirements and responsibilities concerning the protection of secrets. No unit or individual shall release, discuss or disseminate information about state secrets on electronic bulletin boards, chat rooms or network news groups.

For electronic bulletin boards, chat rooms or network news groups that are open to the public, the host or its higher level competent department shall strictly carry out its responsibilities concerning the protection of secrets, establish a complete management system, and strengthen supervision and inspection. If information related to secrets is discovered, it shall take timely measures and report this to the local authorities for the protection of secrets.

The regulations demand that Internet Access Providers

shall provide instruction about protecting secrets as an important part of the Internet related technical training. Agreements and user rules signed between the controllers of national trunk lines and Internet access providers, and between Internet access providers and users shall stipulate clearly that state laws on protecting secrets must be obeyed and that state secrets shall not be leaked.

Article 15 states:

Controllers of national trunk lines, Internet access providers and users shall accept the supervision and inspection conducted by departments in charge of protecting secrets and shall cooperate with them. They shall assist such departments in investigating illegal actions that divulge state secrets on the Internet. They shall also delete information on the Internet that concerns state secrets, as required by the departments in charge of protecting secrets.

Violation of the regulations mentioned above can lead to severe punishment. Content and service providers may face fines or closure, but users found in violation may face the death penalty for posting material that is not to the government's liking. On December 2000, the "Decisions Of The National People's Congress Standing Committee On Safeguarding Internet Safety" stipulated that:

in order to maintain national security and social stability, one who commits any of the following acts, which constitute a crime, will be prosecuted for criminal liability in accordance with relevant regulations of the criminal law:

- (1) Fabricating rumors or slander, or publishing or disseminating other harmful information through the Internet to instigate subversion of state power, overthrow the socialist system, or incite the splitting of the country to damage national reunification;
 - (2) Stealing or disclosing state secrets, information or military secrets through the Internet;
 - (3) Instigating national hostility and discrimination through the Internet to damage national unity;
- Organizing evil cults and contacting cult members through the Internet to damage the implementation of state law and administrative laws and regulations.⁹

In January 2001, possibly as a result of the imminent publication of the *Tiananmen Papers*, the collection of documents about decision-making by senior Chinese officials with regard to the student protests of 1989, the Supreme People's Court set the ultimate punishment:

Those who illegally provide state secrets or intelligence for units, organizations and individuals outside the country through Internet with serious consequences will be punished according to stipulations of the Criminal Law.... in especially serious cases, those who steal, make secret inquiries or buy state secrets and intelligence and illegally provide gathered state secrets and intelligence to units outside the country will be sentenced to ten or more years of fixed-term imprisonment or imprisonment for life and their properties may concurrently be confiscated by the state. In cases of a gross violation of law and where especially serious harm is caused to the state and people, law offenders may be sentenced to death and their properties will be confiscated by the state.¹⁰

PORTALS AND INTERNET CAFÉS

In practice the regulations have led Internet service and content providers and Internet cafés to set up their own monitors. In organizations like Sohu.com, a Nasdaq registered portal based in Beijing, appointed censors are monitoring the chatrooms and the bulletin boards and deleting material mentioned under the eight categories under Article 15 of the September 2000 "Measures For Managing The Internet Information Services." In Internet cafes, managers have appointed people who patrol the monitors checking what material appears on the screen. Both Internet content providers such as Sohu.com and Internet Cafes have issued their own sets of guidelines for users. Sohu.com, for example, gives the following message to clients who want to enter chatrooms:

Please take note that the following issues are prohibited according to Chinese law:

1. Criticism of the PRC Constitution
2. Revealing State secrets, and discussion about overthrowing the Communist government
3. Topics that damage the reputation of the State
4. Discussions that ignite ethnic animosity, discrimination or regional separatism
5. Discussion that undermines the state's religious policy, as well as promotes evil cults and superstition
6. Spreading rumors, perpetrating and disseminating false news that promotes disorder and social instability
7. Dissemination of obscenity, sex, gambling, violence, and terror. Cyber-sex is not permitted within the English chat-room.
8. Humiliating or slandering innocent people
9. Any discussion and promotion of content which PRC laws prohibit

If you are a Chinese national and willingly choose to break these laws, Sohu.com is legally obliged to report you to the Public Security Bureau.

Thank you for your cooperation.¹¹

Personnel of the Beijing-based Feiyu Internet Cafe routinely check screens by walking along the 800 computer units and reading over the shoulders of the clients. A note which is placed on a user's monitor to indicate the start of his or her login time, says "The Feiyu Web Bar Warns its Clients: Please do Not Download Web Pages with Illicit, Violent or Reactionary Content..." Content considered "reactionary" can include Falun Gong-related material, dissident web pages or sites promoting the independence of Taiwan or Tibet. Feiyu's website has a link to all major Internet regulations and added some additional ones. Under these rules, mostly issued by the Bureau of Industry and Commerce, Feiyu management is obliged to turn violators in to the local police station. In December, the *China Daily* reported that police raided the Feiyu Cafe and found some "illegal content," but the management was only fined, and business was back to normal after some hours.

On April 10, 2001, the State Council announced a three-month investigation into Internet cafés and other public Internet service providers. A conference, jointly held by the Ministry of Information Industry, the Ministry of Public Security, the Ministry of Culture and the State Administration of Industry and Commerce, then issued an order saying that within this period, no new Internet cafés would be approved. The moratorium was accompanied by an extensive checking of existing cafés nationwide during which the latter were obliged to re-register. The *Legal Daily* gave what it termed an "incomplete" progress report on June 14, 2001. By that time, police had investigated more than 56,800 "web bars," of which 6,071 were ordered to disconnect from the Internet. Between April and July 2001, over 2,300 cafés had been closed down altogether. Special measures were taken in some provinces. Police in Liaoning province installed software in 13,500 computers in the province's 5,000 Internet cafes to automatically filter pornographic, illicit and other harmful information. The raids were carried out "in order to rectify and standardize the order of the market economy" according to the paper.¹²

INDIVIDUALS DETAINED

Several individuals have been detained as a result of posting material on the Internet. In all known cases they were sentenced under articles in the Criminal Code.

QI Yanchen (36). Sentenced to four years.

Qi Yanchen is one of the founders of the China Development Union, a quasi-nongovernmental organization which was banned in late 1998. Qi was detained in late 1999. In September 2000, the Intermediate People's Court in Cangzhou, Hebei Province sentenced him to four years in prison for posting articles and parts of his book, *The Collapse of China*, on the Internet. The book is critical of China's current social situation. Qi was charged with spreading anti-government messages on the Internet and was convicted after a trial that lasted four and a half hours.

HUANG Qi (36). Trial on hold.

Huang Qi, a computer engineer, was charged with the crime of "instigation to subvert state power." Huang, together with his wife Zeng Li, ran www.6-4tianwang.com, a website designed to find missing persons. On June 3, 2000, authorities in Chengdu, Sichuan province, detained Huang after they deemed the content posted "subversive." On September 25, Huang Qi was

reportedly beaten in detention by three policemen after notes he had taken were confiscated. During the beating, he lost one tooth and got a scar on his forehead, according to a letter he gave to his lawyer in November. On January 2, 2001, the Chengdu City Procuratorate accused Huang Qi of violating Articles 103 and 105 of the Criminal Law. The articles punish actions that involve "organizing national separatism, destroying national unity"; "organizing, plotting or carrying out activities aimed at subverting state political power"; and "overthrowing the socialist system." Huang's trial began on February 13, 2001, but the trial was suspended indefinitely after he reportedly fell ill. It was re-scheduled for June 27, but again postponed. No reason for the delay was announced, nor was a new trial date scheduled.

JIANG Shihua (27). Sentenced to two years in prison.

Jiang was a teacher with the No. 9 Middle School in Nanchong, Sichuan province and owner of the Silicon Valley Internet Cafe in Nanchong. He was detained on August 16, 2000, five days after posting a series of articles critical of the Chinese government on an Internet bulletin board. He was charged with "subverting state political power." The Nanchong Intermediate People's Court sentenced him to two years in prison. In May 2001, a higher court in Sichuan rejected his appeal.

GUO Qinghai (36). Sentenced to four years in prison.

Guo Qinghai, a freelance writer, was arrested on September 15, 2000. On April 3, a court in Cangzhou, Hebei province tried and sentenced him to four years in prison. Guo was charged with "inciting to overthrow state political power." Guo had posted some forty articles on the Internet and published in the Hong Kong based magazine *Kaifang* calling for political reform. No one informed the family before the two-hour trial began, and as a result no family member attended. Guo did not have a lawyer for his defense.

LU Xinhua. Arrested.

Lu Xinhua, the author of several articles published on overseas websites, was detained on March 11, 2001 for "subversion." According to the Information Center for Human Rights and Democracy, Lu was formally arrested on April 20.

YANG Zili (28). Detained (along with Xu Wei, Jin Haike and Zhang Honghai).

Yang Zili, a Beijing based computer engineer, is the founder of the Internet site www.lib.126.com. He was detained on March 13, 2001. Authorities have not given an explanation for his detention as yet. Yang had criticized the crackdown against the Falun Gong on his website. He also used the site to teach people how to use proxy servers, a way to circumvent censorship and access sites blocked by the Ministry of Information Industry.

XU Wei. Detained (along with Jin Haike, Zhang Honghai, and Yang Zili).

Xu, a reporter and a founding member of the "New Youth Study Group," was detained in Beijing on March 13, 2001 for subversion. He was reportedly targeted for his use of the Internet and his association with the study group, which focuses on political reforms.

JIN Haike. Detained (along with Yang Zili, Xu Wei, and Zhang Honghai).

Jin, a geological engineer and a founding member of the “New Youth Study Group,” was detained in Beijing on March 13, 2001 for subversion. He was reportedly targeted for his use of the Internet and his association with the study group, which focuses on political reforms.

ZHANG Honghai. Detained (along with Yang Zili, Xu Wei, and Jin Haikē).

Zhang, a freelance writer and a founding member of the “New Youth Study Group,” was detained in Beijing on March 13, 2001 for subversion. He was reportedly targeted for his use of the Internet and his association with the study group, which focuses on political reforms

CHI Shouzhu (44). Detained.

On April 18, 2001, police detained Chi, a worker in Changchun, Jilin province. They found on him articles with political content which he had downloaded from overseas websites. As of April 2001, he was detained in Lingyuan Prison, Liaoning Province.

WANG Jinbo. Detained.

Wang was taken into custody on May 6, 2001 from his home in Lingyi, Shandong for “libeling police on the Internet” but it is not clear what the content was of his allegedly libelous remarks.

HU Dalin (30). Detained.

Hu Dalin was detained on May 18, 2001, apparently for helping his father, a leftwing essayist named Lu Jiaping, post his writings on websites. The authorities were particularly angry over an article by the father about the case of the U.S. spy plane forced to land in China. The article was posted on May 11, 2001.

LIU Weifang (40). Sentenced to three years in prison.

In June 2001, authorities in Xinjiang Autonomous Region sentenced Liu Weifang, a small business owner, to three years in prison for posting “reactionary articles” criticizing the Chinese Communist Party and its leaders on Internet bulletin boards. He had used his Internet name, lgwf, but authorities traced the messages to him. The *Xinjiang Daily* said Liu got off lightly because he had admitted guilt.

WANG Zhenyong (30). Arrested.

Wang, a former assistant professor of psychology at Southwestern Normal University in Chongqing, Sichuan, was arrested on June 2, 2001 in Shenzhen for downloading and distributing by e-mail promotional material on the Falungong spiritual movement.

LI Hongmin. Detained.

Li, a businessman from central Hunan, was reportedly detained after e-mailing the Chinese language version of *The Tiananmen Papers* to friends. He was detained in Shaoyang, Hunan, as of July 2001 according to the Hong Kong-based Information Center for Human Rights and Democracy.

¹ Agence France Presse, “Jiang Renews Warning Against ‘Pernicious’ Internet,” July 11, 2001.

² Eight separate ministries or government agencies, led by the Ministry of Public Security, are involved in Internet monitoring and control. They include the Ministry of Information Industry, the Standing Committee of the National People’s Congress, the State Council, the Supreme People’s Court, the State Bureau for the Protection of Secrets, the State Administration for Press and Publications, and the State Copyright Bureau.

³ “China to Speed up Internet,” People’s Daily, July 11, 2001. See also China Internet Network Information Center Annual Internet Survey at <http://www.cnnic.net.cn/develst/e-cnnic200101.shtml>.

⁴ PRC Regulations for the Safety Protection of Computer Information Systems (*Zhonghua renmin gongheguo jisuanji xitong anquan baohu tiaoli*), *Fazhi Ribao (Legal Daily)*, February 24, 1994, issued by State Council Order No.147, signed by Premier Li Peng on February 18, 1994.

⁵ PRC Interim Regulations Governing the Management of International Computer Networks (*Zhonghua renmin gongheguo jisuanji xinxi wangluo guoji lianwang guanli zanxing guiding*), *Fazhi Ribao (Legal Daily)*, February 12, 1996, issued by State Council Order No.195, signed by Premier Li Peng on February 1, 1996.

⁶ Management Measures of the PRC Regulations for the Safety Protection of Computer Information Systems (*Jisuanji xinxi wangluo guoji lianwang anquan baohu guanli banfa.*), in *Jisuanji Ji Wangluo – Falu Fagui (Computers and Internet – Laws and Regulations)*, Falu Chubanshe, Beijing: 1999, p. 99. These regulations were published in full by some Internet cafés. See also the website of Feiyu, an Internet café in Beijing at <http://www.feiyu.com.cn/wangba/fagui/jisuanji.htm>

⁷ PRC Telecommunications Regulations (*Zhonghua renmin gongheguo dianxin tiaoli*), October 11, 2000, issued by State Council Order No.291, signed by Premier Zhu Rongji on September 25, 2000. Measures for Managing Internet Information Services (*Hulianwang xinxi fuwu guanli banfa.*), *Fazhi Ribao (Legal Daily)*, issued by State Council Order No.292; signed by Premier Zhu Rongji on September 25, 2000.

⁸ Regulations Regarding Management of Secrets in Computer Information Systems and International Internet (*Jjisuanji xinxi xitong guoji lianwang baomi guanli guiding*), *China Online*, February 2000, [<http://www.chinaonline.com/refer/legal/newsarchive/secure/2000/february/c00012671.asp>].

⁹ Decisions of the National People's Congress Standing Committee on Safeguarding Internet Safety (*Quanguo renda changweihui guanyu weihe hulianwang anquan de guiding*), *Fazhi Ribao (Legal Daily)*, December 30, 2000.

¹⁰ Explanations on Certain Questions Concerning the Specific Application of Law in the Trial of Cases of Stealing, Making Secret Inquiries of or Buying State Secrets and Intelligence and Illegally Providing Gathered State Secrets and Intelligence for Units Outside the Country, in “China: Supreme People’s Court on Stealing State Secrets, BBC Monitoring, January 23, 2001, from Xinhua, January 21, 2001.

¹¹ <http://javachat.sohu.com/english/chat.php3>.

¹² “Police from various regions see success in clearing ‘Web Bars,’” *Fazhi Ribao (Legal Daily)* web edition, June 14, 2001.