



Human Rights and the Internet

In

China

Before the

Congressional Human Rights Caucus

The United States Congress

Presented by

T. Kumar

**Advocacy Director for Asia & Pacific
Amnesty International USA**

Wednesday, February 01, 2006

Thank you Mr. Chairman and members of the Congress; Amnesty International (AI) is pleased to testify at this important and timely hearing. Despite AI's reporting on the issue of Internet censorship and related human rights abuses since 1999, the Chinese Government's determination to crack down on peaceful Internet users seems only to have grown. This trend is disturbing but not surprising, given the Chinese Government's widely acknowledged practice of silencing political dissidents and others who express their views peacefully.

What is new about recently reported abuses is the willingness of U.S.-based companies to join hands with the Chinese Government in aiding such practices.

What does censorship look like in China?

There is a tendency in public discourse to sanitize the issue of freedom of expression and access to information in China, creating the perception that it is simply about not having access to a few controversial websites. This is far from the reality. In China, individuals can be sentenced to death for publishing information on the Internet that the government considers a "state secret" – the definition of "state secret" can change on a daily basis, and can include important public health information (for instance on SARS or HIV/AIDS) or simply an opinion about a labor dispute. Scores of people have been imprisoned in China for using the Internet, and, of those arrested, some have died as a result of torture by the police. Those detained to date range from political activists and writers to Falun Gong practitioners and members of other religious groups banned by the authorities.

Individuals who are active on the Internet, and who challenge the government, can experience continuous harassment. Such harassment includes but is not limited to temporary detention, threats to one's family, business or career, and being followed and intimidated by the police.

Internet companies' assistance to the Chinese Government

Several international companies provide Internet services in China and many have headquarters within the United States. Some of these companies, including Cisco Systems and Sun Microsystems, have helped to build the infrastructure that makes Internet censorship possible while others, including Yahoo!, Microsoft, and Google are increasingly complying with government demands to actively censor Chinese users by limiting the information they can access.

In the most egregious case that we know of, Yahoo! sacrificed the privacy of one of its users to facilitate his subsequent imprisonment for peacefully expressing opinions over the Internet. These companies not only put profits above principle but also willingly ignore international human rights standards. Amnesty International is concerned that, in the pursuit of new and lucrative markets, these IT companies are contributing to human rights violations. Unless a strong action is taken by the U.S. Government and the Congress, this type of practice will not only increase but is likely to move into other areas, which will lead to disastrous impacts on the well-being of the Chinese people and significant risks for U.S. companies operating overseas.

Yahoo denies U.S. Family access to deceased Marine's emails

While American IT companies seem to be falling over each other to help the Chinese Government in censoring its citizens, here in the United States, Yahoo! denied a family access to their deceased son's email, citing privacy concerns. Their son was Justin Ellsworth, a 20-year old Marine killed in November by a roadside bomb while assisting civilian evacuations before a large-scale military offensive against insurgents in the city, said a report in the Detroit Free Press. But when Ellsworth's father John tried to recover his son's email account, he was barred due to Yahoo!'s seemingly unflinching policy of not giving personal user information to anyone besides the account holder. Apparently, this policy is only circumvented when the request comes from one of the world's most repressive governments, with the goal of stifling free speech.

Double standards at home and abroad

There is a tendency in the international business community to deal with the Chinese Government on the basis of a different set of standards. The above mentioned John Ellsworth's case is only one example. Human rights obligations apply to all states equally. Furthermore, nuanced interpretations of international standards on censorship are well documented, including by Amnesty International. This problem extends well beyond the IT sector. Nonetheless, this sector raises particularly troubling concerns, considering how lightly Internet technologies are regulated. When faced with the prospect of challenging the Chinese Government on their repressive practices, companies often claim that the Government is simply too powerful and that they have no alternatives but to comply with their requests, even those that run counter to international human rights norms, the company's mission or standards, U.S. law, or even China's own constitution. If U.S.-based IT companies are to do business in China (or anywhere else), they ought to apply their business standards universally. Another argument we often hear is that the Chinese Government will eventually ease its censorship, and that U.S. companies need to be poised for this imminent change. But there is absolutely no evidence that this is likely to happen. In fact, there is significantly more evidence to the contrary. Though our IT companies like to pretend that there is no stopping the swift march of information in China, we should not underestimate the state machinery of repression so deeply embedded in China's infrastructure. The Chinese Government's investments in Internet controls appear to be keeping pace with technological developments, and for companies to claim that such control is not sustainable for the Chinese is both naïve and dangerous. If we permit American companies to give in to the Chinese on censorship, their infrastructure for control only becomes more

powerful. To ensure that this does not happen, we recommend the development of U.S. legislation regulating U.S. companies overseas, and other companies publicly traded on U.S. stock exchanges (which would include Baidu, the primary Chinese competitor), prohibiting them from complying with violations of freedom of expression and freedom of information by repressive regimes.

Until the time that such regulations are instituted, in situations where companies claim exemption from international standards in order to do business in an emerging economy, those companies should be required to justify their presence in the country and disclose their double standards, while working in a multi-stakeholder process to develop and advance improved standards. As reported widely in the U.S. press on January 31, 2006, Microsoft has publicly stated their hope for the arrival of “a broad set of principles for (the) full range of Internet technology.” We support this recommendation and would expect the process to be open and transparent, including participation by NGOs as well as companies and government, and that it would provide not only principles, but explicit guidelines for implementation and evaluation.

The myth of “net positive” impact

IT companies often point to the “net contribution” that their company’s presence has had on the proliferation of freedom of expression and information in China. While the Internet has undoubtedly increased access to these freedoms generally, there is no evidence we have seen to demonstrate that the presence of U.S.-based IT companies has accomplished any more for the Chinese people than state companies such as Baidu, the leading provider of internet technology in China. If every company operating in China is complying with the same standards of repression, it is hard to understand how using a different company’s search page to find the exact same limited information provides any added benefits to Chinese users. What is clear is that it provides added benefits to the U.S. company, in terms of profits.

Despite their claims, it appears that these U.S. companies are not very concerned about promoting the welfare of Chinese citizens. Take the recent announcements, first by Google and then by Microsoft, that they would provide some disclosure to their users about the fact that their content had been censored “according to local laws and regulations.” As reported in The New York Times on February 1, this new policy would not have prevented the censoring of the Chinese blogger, Zhao Jing. So what is the net benefit of this policy to the Chinese people? They still cannot access information, and they do not learn anything specific about the nature of the censorship, such as which sources were blocked, for what specific aspect of the law. One thing the companies claim is true: each time the disclosure pops up the Chinese users receive a reminder that their government is the primary agent of that censorship (a reminder they probably don’t need). But the message they receive even more clearly is that now America’s most prominent IT companies are partners in that repression, and that they find it acceptable. This is a huge blow for human rights, and for the perception of American values abroad.

We are dismayed that these companies would claim the ethical high ground for a decision that appears to be purely financial. In order for the Internet to fulfill its role as a tool of democratization, a “liberating technology” as Bill Gates referred to it at Davos, companies must UNIVERSALLY ensure freedom of expression is protected and access to information is not suppressed. Where companies cannot, the burden of evidence should be on them to demonstrate the net positive impact of their presence, if such an impact truly exists.

Examples of U.S. IT Companies Aiding Human Rights Abuses

In November 2002, in the report *State control of the Internet in China*, AI cited several U.S. companies – including Cisco Systems, Microsoft, and Sun Microsystems - which had reportedly provided technology used to censor and control the use of the Internet in China. In January 2004 Amnesty released an updated report, *Controls tighten as Internet activism grows*, which indicated that there was a dramatic rise in the number of people detained or sentenced for Internet-related offences, an increase of 60 per cent in 2003 as compared to the previous year's figures. In addition, an unknown number of people remained in detention for disseminating information about the spread of Severe Acute Respiratory Syndrome (SARS) over the Internet. Additionally:

Yahoo!

Also of grave concern are the allegations that Yahoo! has cooperated with Chinese authorities in events which led to the detention of Shi Tao, a Chinese journalist. This case is particularly disturbing because the company provided specific information about an individual user. Linking email to a specific user is information only Yahoo! would have access to, and, seeing as such information was not demanded by a court order, it appears that its release was the result of nothing more than a political demand. Mr. Shi was imprisoned solely for the legitimate exercise of his right to seek, receive and impart information, as guaranteed under Article 19 of the International Covenant on Civil and Political Rights, which China has signed but not ratified. According to the court transcript of the *Changsha Intermediate People's Court of Hunan Province Criminal Verdict*, evidence presented by the prosecutor that led to the sentencing of Mr. Shi included account-holder information provided by Yahoo! Holdings (Hong Kong) Ltd. Yahoo! has admitted that their subsidiary provided this evidence by correcting the record to state that the information was provided not directly by Yahoo! Holdings (Hong Kong) Ltd. but by Yahoo! China, which is held by Yahoo! Holdings (Hong Kong) Ltd. On April 27, 2005, Mr. Shi received a ten-year prison term for sending information about a Communist Party decision through his Yahoo! email account to a website based in the United States. Mr. Shi's appeal was denied on June 2, 2005.

Microsoft

According to recent reports, Microsoft's search engine MSN blocks searches under certain key words, including "democracy", "freedom", "human rights", "Falun Gong", "June 4", and "demonstration", among others. In China, users of the product Microsoft Spaces are also prohibited from using these and other words on weblogs they create. As a result, websites and webpages dealing with human rights, including those of Amnesty International and other human rights organizations, are inaccessible to internet users in China. In January 2006, stories surfaced that Microsoft had cooperated with Chinese authorities in shutting down a controversial blog.

Google

Most recently, Google launched a self-censoring Chinese search engine - the latest in a string of examples concerning global Internet companies caving-in to pressure from the Chinese government. The service curtails the rights of Chinese Internet users to the freedom of expression and freedom of information enjoyed in other countries. Amnesty International's Secretary General, Irene Khan, released a statement from the World Economic Forum in Davos, Switzerland, saying:

"While acknowledging that Google has taken a number of steps to ensure access of Chinese users to the Internet, Amnesty International is nonetheless dismayed at the growing global trend in the IT industry.

"Whether succumbing to demands from Chinese officials or anticipating government concerns, companies that impose restrictions that infringe on human rights are being extremely short-sighted. The agreements the industry enters into with the Chinese government, whether tacit or written, go against the IT industry's claim that it promotes the right to freedom of information of all people, at all times, everywhere."

Our Communications with the Internet Companies:

We have communicated with several IT companies about our concerns, including those named above. So far we have not received any substantive responses from these companies that address our concerns. In many cases these are the same companies that have refused the invitation to attend today's testimony. We are shocked by their willingness on the one hand to collude with the repressive practices of the Chinese Government, and unwillingness to stand accountable in front of the democratic government of their home country.

Overview

Since the commercialization of the Internet in China in 1995, China has become one of the fastest-growing Internet markets in the world. The number of domestic Internet users has been doubling every six months.

With the introduction of the Internet, news reaches China from a multiplicity of sources enabling people to form opinions, analyze and share information, and communicate in ways previously unknown in China. Lively on-line debate characterized the start of the Internet in China. However, the potential of spreading new ideas through the Internet has led authorities to take measures to control its use.

The authorities have introduced scores of regulations, closed Internet cafes, blocked e-mails, search engines, foreign news and politically-sensitive websites, and have recently introduced a filtering system for web searches on a list of prohibited key words and terms.

Those violating the laws and regulations which aim to restrict free expression of opinion and circulation of information through the Internet may face imprisonment and according to recent regulations some could even be sentenced to death. As of January 7, 2004, Amnesty International had recorded the names of 54 people who had been detained or imprisoned for disseminating their beliefs or information through the Internet - a 60 percent increase as compared to figures recorded at the end of 2002. Current information suggests that roughly fifty plus internet-related prisoners continue to be held in China. In addition, an unknown number of people remain in detention for disseminating information about the spread of Severe Acute Respiratory Syndrome (SARS) over the Internet. Prison sentences ranged from two to 12 years.

Internet access expanded considerably in China during 2003. According to official statistics, the number of Internet users had risen to 79.5 million by December 2003 from 59.1 million users in December 2002 - an increase of 34.5 percent. According to the China Internet Network Information Center, the number of Internet users reached 111 million by 2005. This has presented the authorities with greater challenges in their attempts to censor and control the online activities of Internet users. During 2003, there was a growing trend towards assigning greater responsibilities of surveillance and monitoring to a variety of companies in China such as Internet Cafes, Information Service Providers (ISPs) and other enterprises.

Though it appears that Internet activism is continuing to grow in China as fast as the controls are tightened, this should not be misconstrued as evidence that company compliance with state sanctioned repression somehow does more good than harm. Recently, there have been signs of Internet users acting increasingly in solidarity with one another, in particular by expressing support for one another online. Such expressions of solidarity have proved dangerous, as a growing number of people have been detained on the basis of such postings.

The Internet in China - Facts and Figures

- China joined the global internet in 1994. It became commercially available in 1995.
- By 2005, the number of internet users reached 111 million.
- China is second only to the United States in the number of Internet users.
- China's Internet market is likely to become the largest in the world within four years.
- More than 40% of internet users are based in prosperous cities, particularly Beijing, Shanghai, Shenzhen and Guangzhou.
- Internet users are predominantly young, with almost 40% aged 24 or under.
- The proportion of female users continues to increase and now represents over 39 per cent of all users.

- Initially, Internet users were predominantly those with a high school or college education. But those without a college education now make up 68.3% of the total, indicating a broader spectrum of use within China.
- Officials at the Asia-Pacific Economic Conference (APEC) in February 2001 predicted that 70 percent of Chinese foreign trade companies will be able to conduct import and export business via electronic means by the year 2005.
- Since 1995 more than 60 rules and regulations have been introduced covering the use of the Internet.
- In January 2001, a new regulation made it a capital crime to "provide state secrets" to organizations and individuals over the Internet.
- 30,000 state security personnel are reportedly monitoring websites, chat rooms and private e-mail messages.
- Following a fire in a Beijing cybercafe in 2002, the state shut down 150,000 unlicensed cybercafes. Between October and December 2004, China closed over 12,000 Internet cafes.
- On 26 March 2002, the authorities introduced a voluntary pledge, entitled, *A Public Pledge on Self-Discipline for the China Internet Industry*, to reinforce existing regulations controlling the use of the Internet in China. Over 300 Chinese Internet business users have reportedly signed the public pledge, including the U.S.-based search engine Yahoo!
- In July 2002, a *Declaration of Internet Users' Rights* was signed and published by 18 dissidents calling for complete freedom of the Chinese people to surf the Internet.

Imprisonment for Using the Internet

At least 54 Chinese Internet users are imprisoned after often unfair trials solely for peacefully exercising their right to freedom of expression and opinion, in violation of international standards. They include people who have expressed their views or circulated information via the Internet or email. Those detained for downloading information from the Internet, expressing their opinions or circulating information on the Internet or by email include students, political dissidents, Falun Gong practitioners, Tibetan exiles, workers, writers, lawyers, teachers, civil servants, former police officers, engineers, and businessmen.

Signing online petitions, calling for reform and an end to corruption, planning to set up a pro-democracy party, publishing 'rumors about SARS', communicating with groups abroad, opposing the persecution of the Falun Gong and calling for a review of the 1989 crackdown on the democracy protests are all examples of activities considered by the authorities to be "subversive" or to "endanger state security". Such charges almost always result in prison sentences.

Individuals who are active on the internet, and who challenge the government, can experience continuous harassment. Such harassment includes but is not limited to temporary detention, threats to one's family, business or career, and being followed and intimidated by the police. Many of those included in this report have been held for long periods, sometimes for over a year, awaiting a formal trial and for some there has been a long delay between trial and sentencing. All are believed to have been denied full and adequate access to lawyers and their families, particularly during the initial stages of police detention, and several have reported being tortured or ill-treated. In addition, four prisoners directly linked with Falun Gong and charged with Internet related crimes have died in custody. Such violations of the right to a fair trial and to freedom from torture or ill-treatment often contravene provisions of China's Criminal Procedure Law as well as international human rights standards.

The following cases illustrate such failings. They also show how the arrest of one Internet activist can result in spiralling arrests of others who dare to express their support or solidarity online. Several of these cases have been documented by Amnesty International. These cases show the systematic nature of state persecution of Internet activists.

Huang Qi, is notable for being the first person in China to be arrested for posting articles concerning human rights and political issues on his own website. After his trial in August 2001, he continued to be

detained for almost two years before his sentence was finally announced on 9 May 2003 - five years' imprisonment for "inciting subversion". By that time Huang Qi had spent a total of almost three years in detention.

It remains unclear why it took so long for the sentence to be announced after the trial. Huang Qi filed an appeal on May 18, 2003, pointing out that China's Constitution guarantees the right to freedom of speech and of the press. During his appeal hearing, prison guards reportedly held him down by the throat as he tried to speak in his defense. In August 2003 his appeal was turned down and the five-year sentence upheld.

Amnesty International was concerned to note that according to the court verdict, the prosecution cited evidence which included reference to the posting of an Amnesty International document on Huang Qi's website. Amnesty International believes that merely publishing names of individuals imprisoned following the 1989 pro-democracy protests on the Internet can never amount to "inciting subversion".

After his appeal Huang Qi was transferred to Chuanzhong high security prison, in Nanchong in Sichuan Province. Following a visit by representatives of the international non-governmental organization Reporters Without Borders in October 2003, Huang Qi was reportedly placed in solitary confinement and then moved to a punishment cell. He is reported to be in poor health. On June 4, 2005, Huang Qi was released from prison, but remains confined to his parents' home, three hours from his wife and family's home in Chengdu.

- In December 1999 Wang Youcai, founder of the China Democracy Party (CDP), was sentenced to 11 years imprisonment for subversion. Two of the accusations against Wang Youcai involved sending e-mail to Chinese dissidents abroad and accepting overseas funds to buy a computer.
- Lin Hai, a computer engineer from Shanghai, was arrested in March 1998 and is considered to be the first person to have been sentenced for the use of the Internet in China. He was accused of providing 30,000 email addresses to VIP Reference, a U.S.-based on line pro-democracy magazine, and charged with subversion and sentenced to two years in prison in June 1999.
- Members of the Falun Gong spiritual movement, banned in July 1999 as a 'heretical organization', have used the Internet and e-mail to circulate information about repression against the group. Some have been arrested as a result. The Chinese authorities have now shut down the group's websites and blocked overseas websites. At least 14 Falun Gong practitioners have been detained and imprisoned for Internet-related offences.

Amnesty International is concerned about the growing number of individuals being detained, charged and imprisoned for doing nothing more than peacefully expressing their views and opinions on the Internet, including those who have expressed support or solidarity with Liu Di or with detained Internet activists in general. AI continues to call for their immediate and unconditional release.

Amnesty International has investigated the cases of 54 people believed to be prisoners of conscience. They have been detained or are serving long sentences in prison or labor camps for Internet-related offences. Four have died in custody, two of whom reportedly died as a result of torture, and there are reports that others have been tortured or ill-treated in detention.

All were peacefully exercising their right to freedom of expression and opinion. The accusations against them include circulating and downloading articles calling for political and social reform, greater democracy and accountability or redress for abuses of human rights. Most have been charged with "subversion" or membership of a "heretical organization". This latter charge has been used widely against Falun Gong practitioners and members of other Qigong or religious groups banned by the authorities.

Detention of Internet users in connection with SARS

In May 2003 it was reported by the official Chinese News Agency, *Xinhua*, that over 100 people had been arrested for "spreading rumours" or "false information" through the Internet or mobile phone text messages about SARS. Little further information is available about these cases and it remains unclear exactly how many remain in detention. Amnesty International has received reports suggesting that two of them, **Luo Yongzhong** and **Huang Qunwei** were both sentenced to three years' imprisonment for publishing "rumours" about SARS on the web.

Amnesty International recognizes that restrictions on certain rights such as the rights to freedom of expression and association may be justified in certain circumstances, including a public health emergency. However, international human rights law requires that the rights to freedom of expression and association can only be limited in a necessary and proportionate way to achieve some legitimate aim, such as to stop the spread of disease, and the onus is on the government to demonstrate why certain restrictions are necessary. The Chinese authorities have failed to provide an explanation to justify taking the extreme step of depriving people of their liberty in connection with the exercise of the right to freedom of expression in the context of the outbreak of SARS. In the absence of a credible, official explanation for these arrests, Amnesty International considers those detained for 'spreading rumors about SARS' to be detained in violation of their right to freedom of expression.

Amnesty International also notes that the Chinese authorities initially prevented any reporting or open discussion about the scale and impact of the virus, reportedly by blocking websites mentioning the word 'SARS'. As the numbers of those infected rose and deaths were reported, rumors began to spread quickly as people began to panic and search for answers to their questions. Under such circumstances and without access to credible, official information about the disease, it is not surprising that many people resorted to e-mail, chat rooms, bulletin boards and short message texting (SMS). At the time of the SARS crisis, Internet use was reported to have risen by 40 percent and mobile phone use by 30 percent.

In the face of widespread pressure from both domestic and international sources, the Chinese authorities eventually changed their policy to allow more accurate public reporting on the spread of the disease. The World Health Organization pronounced that the outbreak was under control in June 2003. However, a new suspected case of SARS was confirmed in Guangdong Province in December 2003 and first reported by the *Southern Metropolitan Daily* (*Nanfang Dushi Bao*). The authorities have since reportedly questioned the editor and six staff from the paper, apparently over an unconnected issue of alleged corruption. There are concerns that this questioning may in fact be an attempt to intimidate and harass staff involved with breaking the SARS story without official authorization. Amnesty International calls on the authorities to ensure that the media can report freely on SARS, and other issues of legitimate public concern, without fear of intimidation or human rights violations.

Rules and Regulations that Facilitate Crackdown

The provisions set out in the Chinese Criminal Law and the recent regulations provide the authorities with the means to monitor and control the flow of information on the Internet, keep track of users, enforce responsibilities on operators and police, and punish those that violate provisions affecting the Internet.

Scores of administrative regulations governing telecommunications and the Internet have been introduced since 1994. Many update or reinforce earlier regulations as the perceived threats and challenges to the authorities of the Internet grow or change.

Many of these regulations, particularly those concerning "state secrets", are broad and ill defined. Their implementation has often been harsh, resulting in arbitrary arrest, imprisonment, sometimes torture, confiscation of equipment, and heavy fines. Since January 2001, those who provide "state secrets" over the Internet to overseas organizations and individuals may be sentenced to death.

Regulations affecting the Internet have been issued by different Ministries within the State Council (the executive arm of central government), and as the responsibility for implementation has widened, many basic provisions of earlier regulations have been reinforced at different levels. New organizations have also been set up to control the use of the Internet, including the State Council's Internet Propaganda Administrative Bureau, which guides and monitors the content of Chinese websites, and the Ministry of Public Security Computer, Monitoring and Supervision Bureau.

Key Laws and Regulations Introduced Since 1994

Policing the Internet

In 1994, the State Council issued the "*Safety and Protection Regulations for Computer Information Systems*." These regulations gave the Ministry of Public Security (MPS) overall responsibility for "policing" the Internet "*to supervise, inspect and guide the security protection work; investigate and prosecute illegal criminal cases; and perform other supervising duties*".

Monthly Reports on User Statistics

In 1997, the Ministry of Public Security issued some far-reaching regulations, "*Computer Information Network and Internet Security, Protection and Management Regulations*" which were approved by the State Council in December 1997 and elaborated on in more recent regulations.

Under these regulations, all Internet Service Providers (ISPs) and other enterprises accessing the Internet are responsible to the Public Security Bureau. Internet companies are required to provide monthly reports on the number of users, page views and user profiles. Internet Service Providers are also required to assist the Public Security Bureau in investigating violations of the laws and regulations. Serious violations of the regulations will result in the cancellation of the ISP licence and network registration. As a result, some ISPs have introduced self-censoring policies to deal with the implementation of these 1997 regulations, including volunteers, who patrol chat rooms and bulletin boards to ensure observance of the regulations.

Prohibition of the Release of "State Secrets"

On January 1, 2000, multiple articles on the release of "state secrets" were passed:

Article 3: All individuals, legal persons and other organizations conducting international interconnection ("users"), Internet units or access units shall abide by these Provisions.

Article 8: The administration of the protection of secrecy of online information shall adhere to the principle of "those who go online shall bear responsibility." Anyone who provides or disseminates information to internationally networked sites must go through secrecy protection examination and approval. Agencies which implement the administration of secrecy protection examination and approval and relevant units shall establish and perfect online information secrecy protection examination and approval leadership responsibility systems in accordance with national secrecy protection regulations. Units which provide information shall perfect the secrecy protection examination and approval system in accordance with defined working procedures.

Article 9: Anyone who gathers information with the intention of providing online information services shall acquire the approval of the unit providing the information, unless it has already been openly issued in other news media. Anyone carrying out augmentation or updating of online information shall conscientiously enforce a system information secrecy protection examination and verification.

Article 10: Any unit or user who sets up an online bulletin board system, chat room or network newsgroup shall be examined and approved by the relevant secrecy protection work entity, which shall explicitly define its secrecy protection requirements and responsibilities. No unit or individual may disseminate, discuss or transmit information which is a state secret on an online bulletin board system, chat room or network newsgroup. Those persons who set up online bulletin board systems, chat rooms

and network newsgroups which are open to the public or their superior responsible agencies shall conscientiously perform secrecy protection duties and establish sound administration systems to strengthen supervision and monitoring. Upon discovering any information which involves secrets, measures shall be taken in a timely manner and it shall be reported to the local secrecy protection work agency.

Article 11: Users utilizing electronic correspondence to carry online information exchange shall abide by the nation's relevant secrecy protection regulations, and shall not take advantage of electronic correspondence to transmit, transfer or forward on information which is a state secret. Internet units and access units shall explicitly define secrecy protection requirements and perfect administration systems for users of the mail servers which they administer.

Article 12: Internet units and access units shall make secrecy protection education one of the primary components of international interconnection technical training. Contracts entered into between Internet units and access units and access units and users and user manuals shall clearly stipulate provisions that national secrecy protection laws shall be obeyed and the divulging of information which is a state secret is prohibited.

i.e. Highlighted above are particularly chilling aspects of the law, clearly intended to intimidate users (both institutional and individual). The vagueness of the definition of state secrets adds to the uncertainty and needed self-censorship of users.

On January 25, 2000, the Bureau for the Protection of State Secrets issued the "*State Secrets Protection Regulations for Computer Information Systems on the Internet*". These regulations prohibit the release, discussion or dissemination of "state secrets" over the Internet. This also applies to individuals and units when making use of electronic bulletin boards and chat rooms. Operators are under an obligation to report "harmful" content to the local Public Security Bureau. All journalists and writers are required to check their written texts with the state-controlled media before publication.

Amnesty International is concerned that laws and regulations on "state secrets" have been used in the past to imprison people exercising peacefully their fundamental rights to freedom of expression and that the prohibition of "state secrets" in the Internet regulations is yet another way of limiting freedom of expression.

Tough new *Measures for Managing Internet Information Services* were issued in September 2000 by the State Council. "*The Measures for Managing Internet Information Services*" regulate the Internet services and promote the "healthy" development of these services. They also stipulate that all Internet Service Providers (ISPs) and Internet Content Providers have to keep records of all subscribers' access to the Internet, account numbers, the addresses or domain names of the websites and telephone numbers used. ISPs are also required to maintain users' records for 60 days and to provide these to "the relevant state authorities" when required.

These measures draw upon the much broader *Telecommunications Regulations of the People's Republic of China* also issued in September 2000 by the State Council.

Article 15 of these Measures describes information that is prohibited:

- (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 unification;*
- (3) *Information that is detrimental to the honour and interests of the state;*
- (4) *Information that instigates ethnic hatred or ethnic discrimination, or that undermines national unity;*
- (5) *Information that undermines the state's policy for religions, or that propagates heretical organizations or feudalistic and superstitious beliefs;*
- (6) *Information that disseminates rumours, disturbs social order, or undermines social stability;*
- (7) *Information that disseminates pornography and other salacious materials; that promotes gambling, violence, homicide, and terror; or that instigates the commission of crimes;*
- (8) *Information that insults or slanders other people, or that infringes upon other people's legitimate rights*

and interests; and
 (9) Other information prohibited by the law or administrative regulations.

Amnesty International is concerned that the range of information prohibited by this regulation allows the authorities to restrict freedom of expression over the Internet in a broad and sweeping manner which goes far beyond what would be regarded as legitimate restrictions under international standards.

As part of the ongoing effort to control access to information available on the Internet, new regulations were introduced by the Ministry of Information Industry and the Information Office of the State Council on November 7, 2000. These regulations place restrictions on foreign news and the content of online chat rooms and bulletin boards.

According to these regulations, the State Council's Information Office will supervise websites and commercial web portals such as Sohu.com and Sina.com and media organizations may only publish information which has been subject to controls in line with the official state media.

On December 28, 2000, *The Decisions of the NPC Standing Committee on Safeguarding Internet Safety* were introduced. Under these regulations those spreading rumours, engaging in defamation or publishing "harmful" information, inciting the overthrow of the government or division of the country on the Internet will now be punished according to the law. Prison sentences can be passed against those who promote 'heretical organizations' and leak "state secrets".

Below are additional regulations that show the vagueness of state secrets, which are "harmful to national interest". This allows the government to claim anything as being a state secret.

Legislation	Issuer	Selected Provisions
Interim Provisions on the Administration of Internet Publication (2002)	MII GAPP	Article 17: Internet publications may not carry the following types of content: (iii) harming the honor or the interests of the nation; (vi) spreading rumors, disturbing social order, disrupting social stability.
Measures for the Administration of Telecommunication Business Licenses (2001)	MII	Appendix 2 (III)(iv): No operators or their employees shall utilize telecommunication networks to produce, copy, promulgate or transmit any information containing the following types of content: 3. Harming the honor or the interests of the nation; 6. Spreading rumors, disturbing social order or disrupting social stability.
Regulations on the Administration of Publishing (2001)	SC	Article 26: No publication may contain the following types of contents: (iii) harming the honor or the interests of the nation; (vi) disturbing social order, disrupting social stability.
Notice Regarding Further Strengthening the Administration of Periodicals Relating to Current Affairs and Politics, General Lifestyle, Information	GAPP	2. It is strictly prohibited for publications to include any of the following contents: (1) gainsaying the leadership of Marxism, Mao Zedong Thought, Deng Xiaoping Theory; (3) . . . jeopardizing the interests of the nation; (4) . . . influencing social stability; (5) . . . propagating superstition, pseudo-science or incorrect

Legislation	Issuer	Selected Provisions
Tabloids and Scientific Theory (2000)		teachings. (6) spreading rumors, producing and distributing false news, interfering in the broader work of the party or the nation; (7) otherwise violating the propaganda discipline of the party or violating the regulations administering the nation's publishing.
Notice Regarding the Further Strengthening the Administration of Selection of Articles for Newspapers and Periodicals (2000)	GAPP	1 [Newspapers and periodicals] shall not select articles that contradict the guiding policies of the Party and the nation....
Provisions on the Administration of Internet Electronic Bulletin Services (2000)	MII	Article 9: No person may issue any information having the following types of content on an electronic bulletin service: (iii) harming the honor or the interests of the nation; (vi) spreading rumors, disturbing social order or disrupting social stability.
Notice Regarding the Work of Bringing the Periodical Industry Under Control (1997)	GAPP	2(6): In any of the following circumstances where administrative measures have been adopted but there has been no clear improvement, publication should be ceased: (1) Articles have been carried which have severe political errors;
Provisions on the Administration of Electronic Publications (1997)	GAPP	Article 6: No electronic publications may contain the following types of content: (iii) jeopardizing the nation's . . . honor or interests.
Measures on the Administration of Safeguarding the Safety of Internationally Networked Computer Information Networks (1997)	MPS	Article 5: No unit or individual may utilize the Internet to produce, copy, look up or transmit any of the following categories of information: (v) spreading rumors or disrupting social order; (viii) harming the credibility of a government agency.

Internet Licensing System

Licensing laws were passed on September 25, 2000. Article 4: There will be national implementation of a licensing system for commercial Internet information services, and a registration system for non-commercial Internet information services.

No one who fails to be licensed or who fails to comply with registration measures may engage in Internet information services.

Article 14: Providers of internet information services engaged in journalism, publishing and BBS services shall record all information content and the time it was issued, and the internet address or city name; internet access providers shall record information regarding the amount of time each customer was on the internet, the customer's account number, internet address or city name, primary phone number, etc. Providers of internet information services and internet access providers shall maintain these records for 60 days, and shall make them available to all relevant government agencies examining them pursuant to law.

* i.e. even private individuals must register with the government if they want to run a blog, etc. or be shut down or take risk of operating illegally.

Interim Provisions on the Administration of Internet Websites Engaged in News Posting Operations

November 1, 2000. Article 5: The legally established websites of central news units, news units of all departments of the central government's agencies and the news units directly under the provinces, autonomous regions and independent municipalities and the municipal people's governments for the provinces and autonomous regions ("news websites") may engage in news posting operations after receiving authorization. Other news units may not independently establish news websites, but after receiving authorization may establish news web pages and engage in news posting operations on the news website established by a central news unit or a news unit of a province, autonomous region or independent municipality.

Article 7: Non-news units that establish general interest websites ("general interest non-news unit websites") that possess the qualifications set forth in Article 9 of these Provisions, may engage in operations of posting news promulgated by central government news units, the news units of departments of central government agencies, and the news units directly under the provinces, autonomous regions and independent municipalities, but may not post news from their own sources or news from other sources. Other Internet websites that are established by a non-news unit in accordance with the law may not engage in news posting operations.

Article 8: General interest non-news unit websites that engage in news posting operations shall, in accordance with Article 7 of these Provisions, after receiving examination and approval from the people's government information offices for the provinces, autonomous regions and independent municipalities, submit to examination and verification by the State Council Information Agency.

* i.e. no one, or no agency, can transmit any news without formal authorization from the government or a government agency.

The Death Penalty for Offences Related to Use of the Internet

On January 21, 2001, the Supreme People's Court ruled that those who cause "especially serious harm" by providing "state secrets" to overseas organizations and individuals over the Internet may be sentenced to death:

"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."(17)

To date, no prisoners charged with Internet related offenses have been executed or sentenced to death. The ruling is believed to be a reaction to the revelations contained in *The Tiananmen Papers* (18) released in the United States. Extracts of these papers were translated and posted on the Internet.

Order to Monitor Use of the Internet

In January 2001, the Ministry of Information Industry (MII) announced new regulations(19) that require Internet Service Providers (ISPs) to monitor more closely peoples' use of the Internet. Software should be installed to ensure that messages are recorded and if they violate the law the ISP must send a copy to

the Ministry of Information Industry, the Ministry of Public Security and the Bureau for the Protection of State Secrets.

Tough new regulations introduced by the Ministry of Culture restricting access to the Internet and the operations of Internet cafes entered into force on November 15, 2002. Proprietors of Internet cafes are obliged to install software preventing users from accessing information considered "harmful to state security", as well as disseminating, downloading, copying or browsing material on "heretical organizations", violence and pornography. Those aged under 18 years old are banned from Internet cafes. Operating licenses may be withdrawn and fines imposed if these regulations are not properly implemented.

Internet Publishing Provision

On August 1, 2002, the following publishing regulations were passed. Article 6: Engaging in Internet publishing activities may only be done through permission. No unit or individual may engage in Internet publishing activities without permission. No group or individual may interfere with, hinder or disrupt Internet publishing entities in engaging in Internet publishing activities in accordance with the law.

* i.e. In China there is no "free" communication on the Internet, as every posting is considered "publishing".

Bulletin Board Provisions

Starting on November 11, 2002, the following articles came into effect. Article 5: Operators of Internet Information Services who also establish electronic bulletin board services shall, when applying to the provincial, autonomous region, or independent municipality telecommunications administration agency, or the Ministry of Information Industry for a Commercial Internet Information Service License or undertaking registration as a non-commercial Internet Information Service, set forth this fact specifically in their application or registration.

Article 11: Electronic bulletin board providers shall provide only services in accordance with the category or subject matter areas that have been permitted, and may not provide services that exceed these categories or establish other subject matter areas.

Article 13: If an electronic bulletin board provider notices that any information falling under Article 9 of these regulations has appeared on its electronic bulletin board service system, they shall immediately delete it, retain the relevant records, and report it to the relevant authorities.

* i.e. Operators of BBSs must monitor the content and suppress anything that goes against anything the government doesn't like—or risk being shut down, which they often are.

Surveillance Software Mandated in Internet Cafes

On September 29, 2002, regulations on Internet Cafes were passed. Article 23: Units operating Internet Access Service Business Establishments shall examine, register, and keep a record of the identification card or other effective document of those customers who go online. The contents of the registration and records shall be maintained for at least 60 days, and shall be provided to the cultural and public security agencies for examination in accordance with the law. Registration contents and records shall not be altered or destroyed during this period.

* i.e. Internet cafes are required to keep personal information on internet users. They must also monitor what pages users are accessing. Internet cafes are being used as internet police for government.

In October 2003, the Ministry of Culture announced that by the year 2005 all China's 110,000 Internet cafes will need to install surveillance software which would be standardized throughout all Internet cafes

in China. The Ministry of Culture also intends to issue licenses to allow up to 100 companies to manage the majority of Internet cafes. "We are actively pushing an internet cafe technology management system requiring the whole nation to adopt the same standard and each province the same software" said Liu Yuzhu, an official from the Ministry of Culture. According to Liu Qiang, a senior official with the Ministry of Culture, the software would make it possible to collect personal data of Internet users, to store a record of all the web-pages visited and alert the authorities when unlawful content was viewed.

In November, the Ministry of Information Industry (MII) issued rules for approximately 30 large companies that manage Internet addresses in China. While these regulations appear to be intended to improve service standards, they are also aimed at strengthening control over sensitive information posted on the web. According to the MII, such firms must have "strict and effective mechanisms for cleaning bad and offensive domain names, which should be done once a day".

In December, Internet news and information providers, including Renmin, Xinhua, Sina, Sohu and Net Ease, signed up to a new "Internet News Information Service Self-Discipline Pledge". Signatories to the Pledge agree to "obey government administration and public supervision voluntarily, to resist firmly the Internet transmission of harmful information such as obscenity, pornography and superstition, and to resist the substance of information [sic] that violates the fine cultural traditions and moral codes of the Chinese nation".

The introduction of this Pledge echoes similar measures taken in March 2002, when a broader range of companies signed up to the "Public Pledge on Self-Discipline for the China Internet Industry". While Amnesty International recognizes the right of the authorities to regulate the Internet, the vague wording of such Pledges and the lack of definition of key concepts such as "harmful" and "superstitious" allows a wide degree of interpretation. Amnesty International is concerned that these Pledges will be used in conjunction with existing rules and regulations to restrict the fundamental freedom of Internet users to access information or express their views and opinions online.

Implementing the Restrictions

The Internet is a popular and powerful channel for the government and ordinary Chinese to hear each other and to be heard. However, the controls placed on operators and users of the Internet have increased greatly in recent years. This has taken the form of censorship and penalties against all those involved with bulletin boards, chat rooms, e-mail and search engines who contravene the provisions of the Criminal Law and the scores of regulations.

As all communication on the Internet in China passes through government-controlled routers the authorities are able to block access to many sites and to filter content and delete individual links or web pages if considered "dangerous" or "subversive". No list is publicly available on what is filtered and blocked, but a study done by the Harvard Law School on *Empirical Analysis of Internet Filtering in China*, carried out between May and November 2002 and updated on December 3, 2002, found that over 50,000 of 204,000 web sites tested were inaccessible from at least one location in China although some were accessible from the U.S.

1. Blocking

The authorities routinely block news sites, especially foreign-based sites, including those featuring dissident views or banned groups. The blocking appears to be intermittent but more prevalent at times of heightened security such as the anniversary of the crackdown on the 1989 pro-democracy protests, the annual meeting of the National Party Congress or visits from heads of state or government.

Many websites considered to contain politically sensitive information, such as those of human rights organizations and banned groups as well as international news sites, are inaccessible from China. Amnesty International's main website, along with hundreds of others, continues to be blocked. The

average Internet user in China knows there are certain sites that are accessible, searches that cannot be done, or content that cannot be looked at.

In late August 2002, the popular search engine, Google.com, could not be accessed from China for several weeks. Altavista.com was also reportedly blocked. Protest messages were registered on bulletin boards throughout China. In hopes of capturing a larger market of Internet users, most foreign companies operating in China now avoid such confrontations by censoring their search engines (as do the Chinese). Such companies block specific websites on the request of the Chinese government.

2. Filtering

In mid-September 2002, China introduced new filtering systems based on key words, regardless of site or context. Automated technology blocks any communication in which certain banned words appear. Filtering software has reportedly been installed on the four main public access networks in China. Prohibited words or strings of words on websites, e-mail, personal blogs, foreign news sites and search engines are affected. Users trying to access information which includes key words such as 'Taiwan', 'Tibet', 'democracy', 'dissident', 'Falun Gong', 'Dalai Lama', and 'human rights', have continued to be regularly blocked. In addition, several new regulations have created greater responsibilities for control of the Internet through Internet cafes, companies and, most recently, portals providing news.

Filtering technology has largely been provided by Western internet companies, including U.S. based corporations. Among those providing filtering software are Cisco, Nortel Networks, Sun Microsystems, Juniper, and 3COM. Cisco has provided routers to China that can block not only entire websites, but also specific sub-pages, leaving the rest of the site accessible. Groups and individuals in China have used a variety of means to overcome Internet censorship including the use of proxy servers situated outside of China, which circumvent firewalls and the blocking of websites.

3. The Closure of Internet Cafes

Following a fire at Lanjisu Internet café in Beijing in June 2002 which killed 25 people, the Public Security Ministry announced that it had closed down 2,400 Internet cafes in Beijing for safety reasons. Officials in other cities such as Shanghai and Tianjin took similar action. Since then the authorities have introduced a range of regulations affecting Internet cafes, instituted government checks and ordered filtering software to be installed.

While Amnesty International recognizes the importance of health and safety regulations for all public services including Internet cafes, the organization is concerned that the fire at the Internet café in Beijing may have been used as a pretext to crackdown still further on freedom of expression in China.

According to a recent statement issued by the Minister of Culture, there are 200,000 Internet cafes throughout China but only about 110,000 of them are officially registered. All Internet café owners have been obliged this year to re-register with a number of different authorities to obtain a license and avoid being shut down or fined heavily.

Several weeks after the Beijing Internet café fire, the government ordered all Internet cafes to augment their filtering software within weeks and to keep records of all users for a 90-day period. The software prevents access to 500,000 foreign websites, such as foreign newspapers, Falun Gong websites, websites on democracy and human rights and others which are considered "reactionary" or are "politically-sensitive". Those attempting to access these banned sites are automatically reported to the Public Security Bureau. Internet police in cities such as Xi'an and Chongqing can reportedly trace the activities of the users without their knowledge and monitor their online activities by various technical means.

Public Pledge on Self-Discipline for China Internet Industry

In addition to enforcing controls directly, the Chinese authorities are using a variety of means to force Internet companies to take greater responsibility for implementing the numerous laws and regulations controlling the use of the Internet in China. In March 2002, the Internet Society of China issued The Public Pledge on Self-Discipline which entered into force in August 2002.

Signatories to the Pledge agree to:

"...Refrain from producing, posting or disseminating pernicious information that may jeopardize state security and disrupt social stability, contravene laws and regulations and spread superstition and obscenity."

Those concerned with the restrictions placed by the authorities on freedom of expression in China regard the Pledge as another means of censoring certain types of information disseminated on the Internet which is deemed to be politically sensitive.

In July 2002 the Pledge had been signed by over 300 signatories including the U.S.-based search engine Yahoo!. A lawyer working at Yahoo! reportedly stated that Yahoo! will conform to local laws in countries where it operates.

While Amnesty International recognizes that Internet companies should be regulated and that restrictions on their activities may be legitimate, AI is concerned at the wide-ranging and broadly defined nature of this Pledge. The organization fears that this new instrument will be used as part of wider attempts to restrict the freedom of expression and association of Internet users in China.

Internet Freedom and Corporate Responsibility

The rapid rise of the Internet has been greatly aided by the involvement of foreign companies in China. Foreign telecommunications, software and hardware companies are investing heavily in the development of China's Internet.

Amnesty International is concerned at reports that some foreign companies may be providing China with technology which is used to restrict fundamental freedoms.

Sohu.com, a Chinese Internet portal, reportedly funded by overseas companies, and financed by leading investment banks and other venture capital firms from the West, reminds those accessing its chat room that "topics which damage the reputation of the state" are forbidden. "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".

In November 2000, the Ministry of Public Security launched its "Golden Shield" project. This project aims to use advanced information and communication technology to strengthen police control in China and a massive surveillance database system will reportedly provide access to records of every citizen. To realise this initiative, China depends on the technological expertise and investment of foreign companies.

Amnesty International remains concerned that in their pursuit of new and lucrative markets, foreign corporations may be indirectly contributing to human rights violations or at the very least failing to give adequate consideration to the human rights implications of their investments. In its first report on *State Control of the Internet in China*, Amnesty International cited Cisco Systems, Microsoft, Nortel Networks, Websense and Sun Microsystems as reportedly having provided technology which has been used to censor and control the use of the Internet in China.

Following the publication of this report, several companies dismissed allegations that their company's actions might be contributing to human rights violations in China. Cisco Systems denied that the company tailors its products for the Chinese market, saying that "[I]f the government of China wants to monitor the Internet, that's their business. We are basically politically neutral." Microsoft said it "focused on delivering the best technology to people throughout the world", but that it "cannot control the way it may ultimately be used."

Amnesty International considers such responses to be inadequate, particularly in view of recent measures taken at the international level to hold companies more accountable for the human rights implications of their investments. For example the UN Human Rights Norms for Business, adopted in August 2003, state that:

[T]ransnational corporations and other business enterprises shall refrain from any activity which supports, solicits, or encourages States or any other entities to abuse human rights. They shall further seek to ensure that the goods and services they provide will not be used to abuse human rights.

In November 2005, Amnesty International contacted Microsoft and Yahoo! regarding these issues. We urged both companies to conduct their business in China, as elsewhere, in a manner that respects human rights, abides by international human rights standards and avoids complicity in human rights violations. The Internet providers' argument that they are "bringing the Internet to China" is outdated and unacceptable. The Internet already is in China, and such justification should no longer be used when defending their actions. Amnesty International urges all companies which have provided such technology to China to use their contacts and influence with the Chinese authorities to bring an end to restrictions on freedom of expression and information on the Internet and to urge the release of all those detained for Internet-related offences in violation of their fundamental human rights.

Declaration of Citizens' Rights for the Internet

In protest against the measures taken by the authorities to control freedom of expression and freedom of information and association on the Internet, a group of 18 dissidents and intellectuals published a *Declaration of Citizens' Rights for the Internet* on July 29, 2002.

This Declaration challenges the regulations introduced by the authorities and urges the National People's Congress and international human rights organizations to examine the constitutionality and legitimacy of certain regulations. By October 2002 the Declaration had the support of over 1000 web publishers and Internet users.

The Declaration cites the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights and states that,

".....a modern government should be based on the right of individual freedom of speech, the right of organizing associations, the right of questioning government decisions and the right of openly criticizing the government.

....A modern society should be an open society. At the historical juncture of the Chinese nation once again transforming itself from a traditional society to a modern society, any blockade measures are all unfavourable to China's society joining paths with the world and the peace and progress of China's society.

.....Every citizen and government should undertake its responsibility and it has become extremely urgent to safeguard Internet freedom."

One of its signatories, Wan Yanhai, a doctor and web site publisher, was detained on August 25, 2002 on suspicion of "leaking state secrets" and released on September 20, 2002 following international campaigning on his behalf by human rights organizations. He was arrested in connection with publishing a document on the internet detailing deaths from AIDS in Henan Province as a result of selling blood to government-sanctioned blood collectors.

Wan Yanhai worked at the AIDS Action Project, a Beijing-based education and activism group, whose offices were closed by the authorities in June 2002. The web site, (www.aizhi.org) an important independent source of information about the HIV/AIDS crisis in China, had promoted the rights of farmers in Henan Province who had contracted AIDS from selling blood.

On August 1, 2002, Wan Yanhai had circulated an online appeal to all independent Web publishers asking them to join him in protesting against new regulations by giving themselves up to the authorities for operating "illegal" websites. Wan Yanhai had also reportedly made use of Internet chat rooms, discussion and e-mail groups in his efforts to publicise his cause and promote freedom of opinion and expression in China.

Despite the measures introduced by the authorities to stifle freedom of expression over the Internet, the new technology is a cornerstone for economic growth in a country with over a fifth of the world's population. As the importance of the Internet grows so too will the millions of users and the demands of those seeking justice and respect for human rights in China.

Precedent for State Department Support of Voluntary Industry Initiatives

Among our recommendations for the U.S. Government is support (including funding) for an industry-wide voluntary initiative to develop standards for the IT sector as regards human rights. The Government is in a position to support such a voluntary initiative, given the growing presence of U.S.-based IT companies overseas. There is precedent for this type of support by the U.S. Government, including the Voluntary Principles for Security and Human Rights for the extractive industry and the Apparel Industry Partnership, formed on the initiative of President Clinton, which has since grown into the Fair Labor Association.

Conclusion and Recommendations

In conclusion, we feel strongly that the willing submission of U.S. companies to Chinese practices of censorship and related human rights abuses in China presents a challenge which must be faced head on and fast by companies, the U.S. Government and the Chinese Government, in close consultation with NGOs such as Amnesty International.

Amnesty International urges President Bush to:

- Make his position clear on the internet companies' involvement in colluding with the Chinese Government in the Chinese Government's abuse of its citizens. The President should make a public statement condemning China's behavior and the cooperation of IT companies.
- To publicly raise US concern about the crackdown on Internet users in China, during his meeting with the Chinese President Hu's State visit to the United States in April.
- Get a commitment from President Hu on specific benchmarks to improve human rights in China, in the run-up to the Olympics in 2008.

Amnesty International urges Secretary Rice to:

- Make public any assistance the United States Embassy in China offered to IT companies in promoting their businesses in China.
- Make public any issues that were raised with the IT companies about their complicity with the Chinese Government in abusing Chinese citizens' human rights.
- Make public any interventions made with the Chinese Government about these abuses.
- Support an industry-wide voluntary initiative for the IT sector, to develop global standards on human rights. The process should be open and transparent and include stakeholders from business, governments and NGOs, and should lead to not only a set of principles, but explicit guidelines for implementation and evaluation.

Amnesty International calls on the Congress to:

- Initiate a study to fully examine U.S.-based multinational Internet technology corporations' activities overseas.
- Pass legislation regulating U.S. Internet technology companies operating overseas, and other companies publicly traded on U.S. stock exchanges (which would include Baidu, the primary Chinese competitor), requiring them to report on their participation in government-ordered filtering/censorship wherever they operate and prohibiting them from complying with violations of freedom of expression and information by repressive regimes.
- Contact Yahoo! directly, inquiring about the Shi Tao case and Yahoo!'s complicity with China's brutal repression of peaceful political speech.

Amnesty International calls on U.S. companies to:

- Use their contacts and influence with the Chinese authorities to bring an end to restrictions on freedom of expression and information on the Internet and to urge the release of Shi Tao and all those detained for Internet-related offenses in violation of their fundamental human rights.
- Take immediate steps to ensure that all their units – the parent corporation and subsidiaries – stop any actions that could undermine human rights in any country in which they operate, and uphold human rights responsibilities for companies as outlined by the UN Norms for Business.
- Develop an explicit human rights policy, ensuring that it complies with the UN Norms for Business.
- Participate in an industry-wide multi-stakeholder process to develop global principles on IT and human rights, which is open and transparent and includes NGO representatives, and that leads not only to a set of principles, but explicit guidelines for implementation and evaluation.
- Disclose any and all information about filtering/censorship occurring around the world

Amnesty International calls on the Chinese Government to:

- Allow freedom of expression, including on the Internet.
- Release Shi Tao and other Internet dissidents immediately and unconditionally.
- Set a time table to improve human rights in the run-up to the Beijing Olympics in 2008.

Thank you for inviting Amnesty International to testify at this important and timely hearing.

T. Kumar
 Advocacy Director for Asia & Pacific
 Amnesty International USA
 Phone: (202) 544-0200, ext: 224
 Fax: (202)546-7142
 Email: tkumar@aiusa.org

