

Senate Subcommittee on Human Rights and the Law
Committee on the Judiciary

Statement on record

Lucie Morillon,
Washington Director,
and
Clothilde Le Coz,
Internet Freedom Director,
Reporters Without Borders

**Hearing on “Global Internet Freedom:
Corporate Responsibility and the Rule of Law”**

May 20, 2008

Reporters Without Borders would like to thank Chairman Durbin for giving us the opportunity to present this statement on record today, and for taking the leadership on this issue in the Senate.

In this rapidly expansive information age, the new media, including the Internet, has been creating plenty of opportunities for those seeking to enjoy the free flow of information online. Citizen journalists and bloggers have known how to use the power of the Internet. Recently, in Egypt, some officials were sent to jail after reports of torture in Egyptian prisons were posted online. But these opportunities are being offset by increasing repression by authoritarian governments who won't tolerate any expression of dissent. They are ready to do whatever it takes to control the Internet, by filtering it, banning key words, intimidating users—and they are enlisting the help of Western companies to do so. The battle of information is no longer being played out only within the mainstream media. It has taken over the Internet.

As of early 2008, Chinese Internet users became the most numerous web surfers in the world. This situation raises the legitimate issue of the appeal that this huge market they represent will ultimately have (210 million people). Since the start of the 21st century, American Internet sector companies have agreed to sign contracts with the Chinese authorities without the issue of human rights ever being a significant consideration in these negotiations.

In 2005, the Shi Tao case showed the consequences of collaborations between repressive regimes and Internet sector companies. Yahoo! had to concede its share of responsibility in the arrest of this journalist, who, by disseminating information via the Internet, was accused of “subverting the power of the State.” He received a ten-year prison sentence. Yahoo! made it possible for the authorities to identify Shi Tao by disclosing his personal data. The media picked up the story, and Yahoo!'s brand image has been seriously damaged ever since.

Nevertheless, some American companies present in China are still supplying material that allows government authorities to censor the content of certain Internet websites and monitor the Web. Others are adopting rules inconsistent with the freedom of expression that they all claim to uphold as one of their corporate values.

I - A GLOBAL PROBLEM?

Reporters Without Borders is an international press freedom organization. For more than twenty years, we have been striving to defend and promote the right to inform and to be informed around the globe. Because of the success of the Internet, we are seeing freedom of expression violations on the Web every day. Currently, 65 cyberdissidents—most of whom are in China—are behind bars for having exercised their right to be informed and to express their opinions on the Web.

Five years ago, most Internet censorship seemed to be taking place in China and Saudi Arabia. Since then, the trend has spread to other countries. China is not the only country that restricts the circulation of information on the Internet; some 30-odd countries are now practicing some form of this censorship. Reporters Without Borders has designated 15 countries as “enemies of the Internet.” They are: Belarus, Burma, China, Cuba, Egypt, Ethiopia, Iran, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, Vietnam, and Zimbabwe.

The organization also singled out 11 “countries under watch.” They are: Bahrain, Eritrea, Gambia, Jordan, Libya, Malaysia, Sri Lanka, Tajikistan, Thailand, United Arab Emirates and Yemen. Unlike the “enemies,” these countries do not massively imprison bloggers or censor the Internet. But they are apparently sorely tempted to do so, as abuses are common. Many of them have laws that they could use to gag the Internet if they wish, and judicial or political authorities often use anti-terrorism laws to identify and monitor government opponents and activists who express themselves online.

Cases of proven collaboration between Western companies and Internet censors are so far limited to a few countries (see below), but they may well spread if nothing is done. The next Shi Tao case may very well be Vietnamese or Syrian E

II – EXAMPLES OF COLLABORATION BETWEEN AMERICAN COMPANIES AND REPRESSIVE GOVERNMENTS

CHINA

Google is cultivating an ambiguous position in matters of censorship

Google allows users to remain anonymous by concealing their IP addresses, at their request. However, since 2006, the company has agreed to censor the Chinese version of its search engine (google.cn). Google.com is still accessible, but certain content is filtered by the authorities. For example, during the Lhasa demonstrations in March 2008, no headline about Tibet appeared in Google.com’s “News” menu.

However, search engine censorship is a basic freedom of expression issue. According to the most recent study by the China Internet Network Information Center (CNNIC)—an official Chinese agency—72.4% of the information is obtained on the Chinese Network using this type of tool.

It is true that the company has shown more transparency by informing google.cn users that their research results are being screened. However, this disclaimer notice appears regardless of what research is being done. The user therefore does not know what content is really blocked.

unsurprisingly redirected—to baidu.com. Moreover, Chinese authorities are expecting baidu.com to replace every “erroneous” (or censored) page an Internet user may happen to stumble upon.

s of the maps it displays and redesigned borders on the pretext that they pose “a threat to national security.” This measure concerns some 10,000 Chinese mapping websites.

Can we still trust Yahoo!?

The “Shi Tao” case highlighted the role that corporations are playing in Chinese censorship. In 2004, Yahoo! provided the journalist’s IP address to the authorities, which enabled them to arrest him. He was sentenced to 10 years in prison for “illegally divulging state secrets abroad.” In 2007, the company’s CEO apologized to the cyberdissidents’ families before the U.S. Congress, and created a humanitarian fund on behalf of such families, which unfortunately leads us to believe that Shi Tao is not the only one.

Yahoo!’s collaboration was also established in three other cases:

- 1) Li Zhi, a former civil servant, was sentenced in 2003 to eight years in prison. The verdict mentions that the American company Yahoo!, as well as a local competitor, Sina, collaborated with Chinese court officials. It indicates that Yahoo! Hong Kong Ltd and Sina Beijing provided information that enabled the officials to confirm that Li Zhi had created an e-mail account on their websites. It does not, however, indicate whether the content of the messages sent or received by the cyberdissident was also transmitted to court authorities.
- 2) On November 18, 2003, Jiang Lijun was sentenced to four years in prison for “inciting subversion.” He stands accused of having tried to impose democracy by “violent means.” The police considered the cyberdissident to be the leader of a small group of cyberdissidents. According to the verdict, Yahoo! Holdings (Hong Kong) has confirmed that the e-mail account ZYMZd2002 had been jointly used by Jiang Lijun and another pro-democracy activist, Li Yibing. In a paragraph headed “physical and written evidence,” the document also stipulates that a “declaration” dated September 25, 2002 had been found in the e-mail “Drafts” folder associated with this e-mail box, without specifying whether this information had been provided by the California-based company. The access codes could also have been provided by Li Yibing, who is suspected of having been a police informant in this case.
- 3) Wang Xiaoning was sentenced in September 2003 to 10 years in prison for posting “subversive” articles that were distributed over the Internet. The verdict also refers to Yahoo!’s collaboration. This document states that information provided by Yahoo!’s Hong Kong branch helped to establish a link between Wang Xiaoning and messages carried by a discussion forum. It specifies that the moderators of this discussion group hosted by Yahoo! had decided to ban the cyberdissident from using the forum.

In 2007, during a hearing before the U.S. Congress House Committee on International Relations, Yahoo!’s CEO, Jerry Yang, publicly apologized to Shi Tao’s mother, who was present, and decided to set up a humanitarian fund to assist the families of cyberdissidents imprisoned in China.

The company also censors its search engine’s results. In 2002, it agreed to sign a “Public Pledge on Self-Discipline for the China Internet Industry,” pledging to comply with the censorship constraints imposed by the Communist Party.

In the spring of 2008, Yahoo! wrote to Condoleezza Rice to ask that she intervene with her Chinese counterparts in order to secure Shi Tao’s release. This move is one of a few recent encouraging signs that contrast sharply with the attitude of a company which, in 2005, refused to apologize for its actions. Nonetheless, if this admission of responsibility and the measures taken to mitigate the situation represent a positive change in the position of Yahoo!’s leadership, its mode of operation in China does not seem to have changed. From this point on, another Shi Tao case can surface at any time.

During the recent demonstrations of March 2008 in Lhasa, Yahoo! asked for an informant to step forward by directly calling upon Internet users to denounce the Tibetan demonstrators on the “homepage” of their Chinese website. Twelve pictures of Tibetan agitators were posted and Internet users were encouraged to call a phone number connected to a Chinese police department. Within scarcely three hours, one rioter had already been identified and arrested. Another gave himself up.

Can we still trust a company that is willing to collaborate in this way with Chinese authorities and who is helping to worsen the status of human rights in the country by facilitating the arrest of individuals opposed to the regime?

Despite a few noteworthy efforts, Microsoft may be helping to eradicate anonymity on the Web

In 2005, the company agreed to censor its blog tools, Live Spaces, and became the second American company to agree to collaborate with Chinese authorities (after Yahoo!). Words such as “freedom,” “democracy,” or “Dalai Lama,” are filtered and do not appear on these blogs.

After the negative publicity that targeted Microsoft when it announced that it was closing down Michael Anti’s blog, the firm announced two series of measures in 2005:

- It will remove access to blog content only when it receives a legally binding notice from the authorities stating that this content is in violation of local law;
- This content will be removed only in the country in which it violates local law. The blog content will still be accessible to the rest of the world.

In 2008, the company announced that it planned to set up one of its biggest research laboratories in Beijing, which only fuels our fears about the research being done in China. One year earlier, the May 16, 2007 issue of the American magazine *The New Scientist* reported that one of the company’s Chinese laboratories is working on a software program designed to analyze Internet user behavior (based on age, sex, etc.) in order to develop “intuitive” software that will pinpoint the type of Internet user visiting these websites, all for purely marketing and ad-targeting purposes. However, American companies who are claiming their right to carry out this type of procedure simply because they must comply with “local laws,” could be induced to put the websites web surfers visit on file, again by order of the Chinese authorities, but without finding that disconcerting. In fact, Chinese authorities are striving to eliminate anonymity on the Internet, and this type of research is helping them to do just that.

On May 22, 2007, the Internet Society of China (ISC) asked several local and international companies to sign a “self-discipline code” to encourage cybernauts to identify themselves, and which all local search engines have applied—including Microsoft and Yahoo.cn, even though they stated that they would refuse to apply the clause requiring Internet users to register their online visits.

Cisco contributed to the root of Chinese censorship

This company has sold routers (a software or hardware tool for directing data through a network linking several servers) to the Chinese government that censor certain Internet website addresses. Despite this technological involvement, which can adversely affect the company’s image, the shareholders refused to vote for a resolution in 2006 which asked that a report be published within six months, at nominal cost, establishing a list and an evaluation of the practical measures that the company might reasonably take to reduce the probability that its business practices could lead to more human rights violations—particularly those involving freedom of expression, and cause more fragmentation of the Network.

Several months prior to Cisco System's General Meeting, at a hearing before the House of Representatives' Committee on International Relations, Mark Chandler, Cisco System's Senior Vice President and General Counsel had stated: "*Cisco sells its products, including Internet and surveillance technology, primarily through resellers, to government agencies and state-owned entities throughout the world. The U.S. State Department and others have documented how various governments, including several governments with which our Company does business, monitor, censor and jail Internet users, through manipulation of Internet technology.*"

Cisco Systems explains that it is not responsible for the way some products are being used. However, the company helped to build the Chinese Internet and some people are wondering what role Cisco's technicians may have played in setting up the Chinese Web's surveillance arsenal. An equipment contract of that magnitude rarely comes along without a comprehensive technical assistance contract.

IRAN

Paradoxically, the embargo that the United States has chosen to enforce against this country in view of the Iranian refusal to suspend its sensitive nuclear activities, is involving Americans in the Iranian censorship game. More and more American companies are withdrawing from the market because of the economic sanctions adopted by the UN in October 2007. For example, Iranian websites are more infrequently hosted by foreign servers, so they are now easier to censor. Likewise, cybernauts have access to Webmails less and less often (even though they are harder to monitor), because Iran is categorized as a "dangerous country," with which no one should deal.

In November 2007, **Yahoo! and Microsoft** removed Iran from their list of Webmail services, which are more difficult to monitor than traditional mail accounts controlled by a local server. Gmail (Google) is still accessible.

Godaddy, a web hosting and Internet domain name registrar, has had its participation in the Iranian market on hold since 2005 as a result of these sanctions. By deciding to no longer host Iranian websites, American companies are forcing them to rely on Iranian hosting companies, which are much more strict about censoring content.

Most of the opposition Internet websites are hosted by foreign companies because they cannot be legally banned, since their servers are based abroad. They can only be filtered.

Furthermore, the filtering technologies are supplied by **Secure Computing** (San José, California), via "SmartFilter" software that allows users to block Internet website addresses. According to Secure Computing, this software makes it possible to block millions of websites in over 60 categories. It is therefore easy for the Iranian government to block websites for political reasons. "SmartFilter" is programmed to block websites hosted abroad as well as locally. (Beware: according to Secure Computing, the company has never sold an ownership license to Iran, so the government may be using it illegally!)

VoIP.ms (an Internet-based cell phone service) does not register the IP addresses of Iranian users because of the economic and financial sanctions imposed by the UN.

The company **Websense, Inc.** (San Diego) supplies filters used by the main Iranian ISP, ParsOnline.

YEMEN

According to the Open Net Initiative team's tests, Websense software (San Diego) is used by Yemeni authorities. The extent of the company's involvement is unknown. Is Yemen using its product legally or not? Yemen's main ISP, TeleYemen, blocks websites corresponding to the

categories “content reserved for adults,” “gay, lesbian or bisexual,” “sexual education,” as well as the majority of contents classified as “adult.” But TeleYemen also has a category called “user-defined,” that allows other sites to be blocked on the basis of other criteria.

Yemen is an example of those countries who could restrict the Internet in the near future and where the use of US products have been taken out of the hands – and control – of the American companies.

It has been said the presence of Western IT companies in authoritarian countries can help open up their societies. It is true, as far as these companies set higher standards in terms of freedom of expression than their local competitors. This is not a case of business as usual.

III - CONSEQUENCES OF THESE ETHICAL FAILURES

We believe that these practices violate international law and the right to freedom of expression as defined in Article 19 of the Universal Declaration of Human Rights, which was proclaimed by the United Nations when it was founded and is meant to apply to everyone—business corporations included.

Such ethical failings on the part of American companies damage the image of the United States abroad. Access to Voice of America and Radio Free Asia’s websites, whose funding comes from the IBB, has been regularly blocked on the Chinese version of Yahoo! and Google. These companies owe U.S. taxpayers an explanation for why and how their money is being used to pay for the consequences of these firms’ collaboration with China’s censors.

Internet companies were created to facilitate information access for all. Yet some companies now find themselves in the awkward position of collaborating with Web censors in an effort to alter the very nature of the product they are selling. By collaborating with repressive regimes’ censorship policies, they are helping to create country-specific access to multiple versions of the Internet. They are putting borders on this universal arena of communication that the Internet was intended to be.

The Internet is used in China to channel and influence public opinion, especially in support of nationalistic sentiments, against China’s enemies, and to promote Communist Party propaganda

Internet censorship in China subverts U.S. diplomacy efforts to promote democracy in the world. By helping Chinese authorities to crack down on dissidents and control the free flow of information online, some U.S. IT companies are indirectly helping to block political changes in the country, thereby preventing China from following the path to democracy.

Business decisions made about markets based in Internet-restrictive countries cannot brush aside the issue of human rights if we want to prevent U.S. companies from being turned into a tool for repression. How can American companies still do business in China without compromising international standards for human rights or the viability of their operations? There are no miracle solutions, but the recommendations listed below should help them stand their ground on the issue of user privacy and basic human rights. We believe the fear of being thrown out of the Chinese market is overstated. The Chinese authorities still need the know-how of these major IT firms and there are reasons to believe that they would not dare take measures that would be seen as business-hostile, and thereby compromise investors’ trust.

IV - RECOMMENDATIONS

At the technical level:

- An appropriate filtering policy

Any Web-filtering measure is typically introduced because of a security concern (parental filter, for example). This is one of the reasons why it is easy to find them on the market. Couldn't the companies that sell these software programs to repressive countries design them in such a way that certain words such as "democracy," or "human rights" could not be filtered, thus guaranteeing that their users can access at least a minimum amount of information?

- Development and better publicity of user empowerment tools to get around censorship.

Companies could help already-existing software whose developers lack the necessary funding (Psiphon, TOR) to become more accessible (by advertising them, providing links on their homepages, or just by financing research for these projects). Creating a fund to promote research on ways to bypass Internet censorship would allow this problem to be addressed and demonstrate the companies' good faith and their desire to ensure that information can truly continue to circulate freely on the Net.

At the policy level:

These companies need to adopt a self-regulation policy and incorporate provisions in their methods of operation which will guarantee the respect of international human rights standards. Some of the provisions that should be taken into account are:

- a ban on having local servers in repressive countries;
- agree not to store personal data that would allow Internet users to be identified on the very territory of countries that refuse to respect freedom of expression on the Internet;
- agree not to be "proactive" in matters concerning censorship;
- legally challenge the requests of authoritarian regimes (ask for written legal binding requests).

The adoption of a voluntary set of principles by ICT companies would bring us a lot closer to realizing these goals than a multitude of individual initiatives.

Discussions between some of the companies, academics, NGOs and stakeholders have been going on for about 2 years, facilitated by nonprofit business associations Business for Social Responsibility (BSR) and Center for Democracy and Technology (CDT). The success of these discussions is as yet uncertain. The companies should not only agree on how to legally challenge government requests that could potentially violate human rights and users' privacy, but also allow an independent monitoring procedure to assess the latter's compliance with these principles. Cisco Systems is not part of this process.

Any voluntary set of principles, however, would not prevent another Shi Tao case from happening, for even if the companies can challenge the requests—by asking for written requests instead of just a phone call, for example—they are still facing governments that require them to abide by local laws. Some companies complain that this is a government-to-government issue. They need a shield that will protect them from being directly answerable to governments. The Global Online Freedom Act (GOFA) introduced by Representative Chris Smith (R-NJ) would do exactly that: put the U.S. government directly between U.S. companies and the Chinese government. Requests about these companies' users' information would have to go through a process vetted by the U.S. Justice Department and inquirers would have to prove that this is a legitimate law enforcement issue. The number of requests coming from authoritarian governments would then very likely drop, and they would have to find another way to go after dissidents—*without* the complicity of U.S. firms.

Other interesting provisions of the bill would require the U.S. companies concerned not to locate the servers containing personal identifying data in territories controlled by such governments, putting them out of these countries' jurisdiction. The companies would also have to act transparently and transmit information about the type of censorship they apply to an interagency-

staffed Office of Global Internet Freedom, whose job it would be to define U.S. government policy for the promotion of the free flow of information online and to monitor violations. The bill also calls for the drafting of a voluntary code of conduct. Companies that do not comply with the GOFA's provisions—especially with regard to the protection of user data—would be sanctioned. The GOFA would also provide for a feasibility study to control the exporting of equipment, software and applications sold by U.S. Internet sector companies to countries the White House designates as repressive.

Senate legislation addressing the same issues as the GOFA—especially the issue of personal identity data protection—is crucial to preventing American companies from being forced to collaborate with repressive regimes in their dissidents' witch hunt.

Reporters Without Borders is ready to offer its assistance to you and to this subcommittee on this important issue.