



Reporters Without Borders USA

Washington DC bureau
1500 K Street, NW, Suite 600

Washington DC, 20009

tel: 202 256 56 13

luce.morillon@rsf.org

www.rsf.org

Tom Lantos Human Rights Commission
U.S. House of Representatives

Testimony of Lucie Morillon,
Washington Director
Reporters Without Borders

Hearing on "Internet Censorship"

June 18, 2009

Mr. Chairman and Members of the Commission:

Thank you for giving us the opportunity to present our testimony today on the global trends in Internet censorship.

These past days, the events in Iran have been a reminder of the importance of alternative sources of media in closed societies. Some say Twitter has been to the Iranian events what CNN was for the Tiananmen square massacre in 1989.: a platform to reach the rest of the world. It illustrates the growing influence of online social-networking services as a communications media. A media used by the opposition, but also citizen journalists and rights activists to unify their supporters and get their messages through while foreign news coverage has been limited by Iranian government restrictions barring journalists from "unauthorized" demonstrations.

Internet as a tool for freedom – Importance of alternative sources of media in closed societies

The Internet offers a tremendous potential for openness and freedom. In heavily censored countries, it has provided a space for discussion and debate that had been non-existent or limited in mainstream media or society. It challenges authoritarianism, empowers individuals as never before and bolsters the exchange of information that makes an important difference in people's lives.

Traditional media organizations have not always been able to expose human rights abuses in repressive countries. In 1988, the world received little notice of the riots occurring in Burma and the military junta's subsequent violent crackdown on demonstrators. News of these events only reached most Western countries weeks if not months after they occurred.

With the help of the Internet and non-traditional media, the blatant human rights abuses that occurred during Burma's 2007 Saffron Revolution were widely covered. Compelling YouTube footage, often filmed by citizen journalists on cell phones or inexpensive low-resolution cameras, was conveyed around the globe, sparking international outrage. While Burmese authorities eventually shut down the Internet in order to continue their crackdown on dissidents unabated, the news was already out.

In China, activists and regular citizens have used the Internet to discuss issues such as consumer rights, social rights and environmental concerns. The blogger Zola for instance, has become a spokesperson for the conditions of Chinese workers and has compelled the traditional media to follow his lead and stop ignoring this topic. As a result, Internet has been responsible for improving the quality of traditional news coverage. Internet users also criticized the distribution of aid after the Sichuan earthquake and their calls for national mobilization ultimately forced Chinese authorities to address the issues at hand.

In Saudi Arabia, women enthusiastically took to the Internet and were able to express themselves freely and discuss health issues until the authorities, claiming to be fighting the promotion of pornography, blocked them.

In Egypt, policemen were prosecuted after a video circulated on Internet, showing them torturing a suspect.

Not only a space for expression, the Web has also become a means for action, particularly through social networking sites.

In Egypt, these sites have taken on the role of trade unions, which have been banned under a state of emergency law in place since 1981. Active Internet users create virtual rallies that can give rise to genuine political demands. One group, created on Facebook, boasts more than 65,000 members and was used to channel protests in April 2008. Calling on Egyptians to "stay home", it contributed to a general strike and one of the largest expressions of civil unrest in several years.

In Iran, the fight for women's rights, insufficiently covered by the traditional media, was taken to the Internet with the campaign "One million signatures for the abolition of discriminatory laws against women". This ensured it high visibility on the international scene.

The demonstrations that followed the Iranian presidential elections have also been widely covered on social networks. Anyone wanting to follow the situation closely had better read blogs, watch Youtube and keep an eye open for minute-by-minute Twitter updates from a country with a young and Internet-savvy population.

The new media involvement grew in response to the lack of coverage from the foreign media at the beginning of the crisis and eventually helped coordinate the opposition's demonstrations. While the government tried to limit communications, new kinds of social media and technical innovations are allowing Iranians to find new ways around the restrictions. "IranElection" was the top Twitter trend of the day last Monday, June 15.

Repressive governments' counter offensive

Repressive governments have fought back against these developments, using different tools to silence dissent. At least three dozens countries are currently involved in some kind of Internet filtering and censorship.

- Some of them have set up of very sophisticated system of Internet censorship and filtering, China being the world champion of such tactics.

- As of today, 68 cyberdissidents and bloggers are currently in jail for expressing themselves freely on the web, some of them sentenced to more than 20 years in jail. These detentions as well as further restrictions on Internet access have been used as means to intimidate other users. In 2007, after having criticized his country's religious authorities and President Hosni Mubarak, Egyptian blogger Kareem Amer was sentenced to three years in prison for "inciting hatred of Islam" and one year for "insulting" the Egyptian president.

- Legal proceedings have been used against bloggers, sued for "endangering national security", "libel" or "insulting a head of State".

- In order to counter dissidents, many governments have utilized the Internet to spread misinformation and propaganda. In a bid to limit online criticism before the Beijing 2008 Olympics, the Chinese government paid Internet users to leave pro-governments comments online. Called the "Fifty cents" – an ironic reference to the money paid for non-spontaneous comments, Chinese authorities contributed to the manipulation of news and information.

Reporters Without Borders issued a list of "Internet enemies" last March, that included Burma, China, Cuba, Egypt, Iran, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan and Vietnam. These countries have transformed the Internet into an Intranet, preventing users from obtaining news seen as "undesirable".

Resourceful Internet users

However bloggers and Internet users have proven to be resourceful. For instance they will often misspell a keyword they know is censored in order to avoid having their posts deleted. For these reasons, the Chinese authorities ended up blocking about 500 keywords related to Tiananmen Square.

They also use metaphors to get their message through. This is why the term River Crab was created by netizens in China, in reference to Internet censorship. In Mandarin, the word River Crab sounds similar to the word harmonious. Because the Chinese Communist Party announced the goal of constructing a "Harmonious Society", as an excuse to delete negative news, Chinese netizens use the name River Crab to describe the actions of blockading and concealing negative news.

Internet users often employ proxies, or software and technologies such as Freerate, VNP, Tor or Psiphon to bypass censorship. According to the New York Times, The Global Internet Freedom Consortium, an Internet proxy service with ties to the banned Chinese spiritual movement Falun Gong, offers downloadable software to help evade censorship that is being used in Iran.

In countries where access to news is prized, it is not unusual to find software designed to defeat online censorship already installed on computers in cybercafes. Internet experts constantly create and fine-tune software version so as to adapt them to the reality of the virtual world. Once censors have identified proxies, new ones become available almost immediately, transforming internet use into constant game of cat and mouse between government and citizen.

Western IT companies making it easier for Web censors

Human right defenders should remain very vigilant about these developments and not take Internet freedom for granted. Some governments invest a lot of resources in Internet censorship and not everyone is tech-savvy or able to go around Internet censorship and make the effort to find independent information. Repressive governments such as China have even made their jobs easier by enlisting the help of Western companies to control the Internet. Yahoo and Google censor the results of the Chinese version of their search engines to remove content deemed sensitive by the Chinese authorities and Microsoft has censored the Chinese version of its blog platform.

Secure Computing has also sold Tunisia technology that allows it to censor independent news and information websites.

Today, most young people in China do not know what happened on June 4th, 1989, proof of how effective media and Internet censorship has been. Of course there is still a way to find such information online, but you have to know what you are looking for.

Yahoo has gone farther than most other companies and given authorities personal identifying information on users that has allowed the Chinese authorities to identify and convict at least 4 dissidents who expressed themselves freely on the Web. One of them is Chinese dissident Shi Tao. When dissidents initially choose a webmail-based account, they should be entitled to better privacy protection from a multi-national company than the local ISPs directly controlled by the government.

The next challenge for the companies will be Vietnam. More than 80 % of Vietnamese Internet users are hooked up to the American companies Google and Yahoo. The ministry of information and telecommunications is planning to put forward co-operation proposals to regulate the content of blogs using foreign companies' platforms, under which they would have to accept to provide information about their customers.

Reporters Without Borders has been asking IT companies not to host their e-mail servers within an Internet-restricting country to avoid being forced to reveal the identity of their users.

China has recently gone one step farther in enhancing its Internet censorship system. It announced earlier this month that personal computers sold from July 1st must carry Internet-filtering software pre-installed by the manufacturer, actually allowing the government to spy on individual users and preventing them from accessing an ever-changing list of banned websites. Concerns have been expressed that the software is full of flaws that could expose users to hackers able to steal personal information. Western PC manufacturers have since asked the Chinese government to reconsider its decision. The Chinese blogosphere has been abundantly commenting on how to

deactivate the software. US computer makers should lend them a hand.

Despite resourceful netizens, the fight for a free Internet is far from being won, in front of powerful governments ready to implement “Big Brother”-like policy. Concrete measures could help sustain the efforts of cyberdissidents in closed societies so that the Internet can remain an open window to the world when all the other windows have been shut.

Recommendations:

- The US authorities should allocate more resources to groups who are drafting software and technologies to by-pass Internet censorship.
- The US should build an alliance of countries that would raise the issue of Internet censorship before the WTO, considering that the lack of information is a barrier to free trade
- Congress should continue holding hearings about Western companies collaborating with Internet-restricting countries, especially since representatives of companies such as Cisco Systems have not joined in the industry’s discussions that led to the creation of the Global Network Initiative
- Congressional hearings should be held as soon as possible with US PC makers to discuss new regulations, how to avoid implementing repressive measures as well as look at the claims that the Green Dam software contains pirated code from a California company.
- Congress should pass the **Global Online Freedom Act (GOFA)** introduced by Rep Chris Smith from New Jersey as soon as possible. This bill aims to prevent US companies from “cooperating with repressive governments in transforming the Internet into a tool of censorship and surveillance.” A similar initiative is being considered by the European Union.

Inspired in part by the Foreign Corrupt Practices Act, it also aims to ensure that the US government fulfils its responsibility “to promote freedom of expression on the Internet” and “restore public confidence in the integrity of US businesses.”

If adopted, this bill will be a significant advance for online free expression and the best way to avoid another Shi Tao case. Companies cannot combat censorship on their own. By turning the US government into a referee, the GOFA’s new version is an alternative solution that prevents US companies from being accomplices to the violation of international standards on protection of free expression.

Under the new version of the GOFA, US companies operating in repressive countries would be required to keep a record of any request made by the government of that country for the identification of an Internet user, together with a record of the company’s response to the request. This information would have to be passed to the US justice department which, if it questioned the request’s legitimacy, could order the company to refuse. Companies that did not comply with the law could be fined.

Like the previous version of the GOFA, approved by the House foreign affairs committee on 23 October 2007, the new version would forbid US Internet companies from keeping client information on servers located in repressive countries. It also provides for a study to determine the feasibility of imposing export controls on products that could be used by repressive governments to control the Internet.

If the GOFA is adopted, US companies will no longer be able to censor US government websites or US government-sponsored websites abroad, and will have to act with transparency. Information about any Internet filtering they implement will have to be passed to an Office of Global Internet Freedom, which will have the job of defining US government strategy for promoting the free flow of information online and monitoring violations.

The Office of Global Internet Freedom will be able to order a US company to refuse to cooperate with a request from a foreign government if it does not consider the request to be "legitimate" or in compliance with existing legislation governing the disclosure of personal information.