

**WRITTEN TESTIMONY OF MORTON SKLAR,
FOUNDING EXECUTIVE DIRECTOR EMERITUS (RETIRED),
WORLD ORGANIZATION FOR HUMAN RIGHTS USA***

**COMPLICITY OF U.S. CORPORATIONS IN INTERNET
HUMAN RIGHTS ABUSES BY THE GOVERNMENT OF CHINA
AND OTHER REPRESSIVE REGIMES**

**SUBMITTED TO THE
SUBCOMMITTEE ON HUMAN RIGHTS AND THE LAW
OF THE JUDICIARY COMMITTEE OF THE U.S. SENATE
HEARING ON MARCH 2, 2010**

Contact: mshumanrights@verizon.net; telephone: (301) 946-4649

* This testimony is provided in a personal capacity, and does not necessarily represent the official views of Human Rights USA

Senator Durbin and Members of the Committee:

The problem that Google brought to public attention a few weeks ago concerning cyber-attacks by Government of China agents against a large number of U.S. government agencies and corporations is just the tip of the iceberg with respect to China's multifaceted electronic monitoring activities that result in major human rights abuses and national security violations, both in their own country, and in the United States. The significant role that U.S. companies have played in facilitating electronic surveillance activities by China and other highly repressive regimes around the world, including Iran, through the provision of Internet user information and the export of products and technologies that build foreign electronic surveillance capacity, should be profoundly troubling for the American people, and deserves considerably more attention than it has received.

To its credit, the U.S. Congress has for a number of years sought to bring attention to this problem. This Committee under the leadership of Chairman Durbin, as well as the House of Representatives Human Rights Subcommittee of the Foreign Affairs Committee under the leadership of the late Congressman Tom Lantos and Co-Chair Chris Smith, have held a series of hearings on these issues, including those held in February, 2006, bringing representatives of Yahoo!, Cisco Systems and other U.S. companies before Congress in an effort to find out more about how their actions and policies are helping to make Internet surveillance and repression possible. These hearings have helped to reveal the sad fact that, in direct violation of U.S. laws, and fed by the profit motive, Yahoo!, Cisco Systems and many other U.S. companies have provided significant support and assistance that has facilitated major human rights Internet abuses in China, and in other repressive regimes such as Iran.

This Committee's hearings of May 20, 2008 revealed that Cisco Systems had marketed and sold Internet routers to Chinese law enforcement agencies with the articulated purpose of helping Chinese officials identify, arrest and persecute political dissidents and religious minorities (Falun Gong practitioners in particular) in violation of U.S. export control laws that prohibit all sales and exports to China that served law enforcement purposes and that could be misused to promote human rights abuses (the Tiananmen Square provisions of the Export Administration Act). Hearings on the House side in November 2007 brought considerable pressure to bear on Yahoo! for improperly providing Internet user information to Chinese authorities that resulted in the arrest of Shi Tao and hundreds of other Chinese who lawfully and peacefully used the Internet for free speech and democracy support purposes. As a result of those hearings, Yahoo! settled a lawsuit filed on behalf of Shi Tao and detainees in Chinese prisons who were arrested and tortured as a result of Yahoo!'s complicity,

brought by the human rights group that I founded and headed for many years (Human Rights USA).

But sad to say, the problem has not been resolved by these several Congressional hearings, the successful Human Rights USA lawsuit, and the substantial media and public attention that has been brought to bear on the issue of the participation and facilitation of major U.S. internet companies like Yahoo! and Cisco in human rights abuses involving the Internet. Neither have any concrete results been achieved through the voluntary effort by several U.S. companies to develop a Code of Conduct for business practices affecting the Internet (the Global Network Initiative). It is noteworthy that Cisco Systems, for one, did not even see the value of participating in the Internet industry Code of Conduct initiative, and has refused to endorse the resulting Code. As has become clear through the hearings of this Committee and through other means, Cisco has been selling Internet equipment and technology to China law enforcement agencies in direct violation of U.S. law and the industry Code of Conduct, and encourages these sales by suggesting that they would enhance China's capability to monitor Internet use and electronic communications so as to identify and track dissidents.

The time has come for the U.S. Congress to act in a more forceful way to make certain that U.S. companies are no longer permitted to facilitate persecution by making electronic surveillance possible through the provision of U.S. products and technologies. Nor should the U.S. Government continue to fail in its duty to properly monitor and enforce the export control laws with respect to Internet technology and human rights abuses. We urge Congress to pursue these types of hearings even more forcefully, and on a broader basis, and to adopt legislation along the lines of the Global Online Freedom Act, that will help to ensure that U.S. companies like Yahoo! and Cisco are not permitted to facilitate major human rights abuses by repressive governments involving the Internet and electronic surveillance.

As we have indicated, the problem is not restricted to U.S. companies such as Yahoo! and Cisco providing Internet information and monitoring technologies to repressive governments in direct violation of U.S. law and ethical standards. The Bureau of Industry and Security of the U.S. Department of Commerce shares responsibility, as they have not properly monitored and enforced compliance with U.S. export control laws – specifically the Tiananmen Square provisions of the Export Administration Act – to identify, prevent, and impose sanctions on violations. Just one week ago BIS issued a new Compliance Guide that for the first time provides much clearer standards for U.S. companies to apply to their marketing and export practices. This was an important first step. But it remains to be seen whether, in practice, the profit motive of the companies, and the balance of trade, political, and foreign policy concerns of the U.S.

Government, will be allowed to override the Tiananmen Square prohibitions and other human rights standards incorporated in U.S. laws and policies.

The situation involving Cisco Systems' sales in China, discussed in the May 20, 2008 hearing of this Subcommittee in which Cisco's General Counsel Mark Chandler appeared and testified under oath before Congress, provides an excellent case in point.

As your hearings indicated, Cisco sells routers and switches to the Chinese government for use in various public sectors including that of the police and security forces. [p. 17 re: PSB]. Cisco has consistently claimed that these are "off the shelf" products that could be purchased elsewhere, and that they are "dual use," or "neutral" products that are not necessarily geared to prohibited uses under U.S. law. However, this overlooks several obvious points. First, Cisco made a determined effort to market these items to law enforcement entities in China, and Cisco geared its sales pitch to the use of these items for law enforcement purposes – specifically, the monitoring of Internet use and electronic communications, which in turn was used to identify and punish political dissidents and religious minorities for their free speech and free exercise of religion rights. As such, these sales efforts and actual exports violated U.S. law on its face, since they are prohibited on an outright basis by the Tiananmen Square provisions of the Export Administration Act.

Second, Cisco was not making these sales pitches and exports to Chinese law enforcement agencies in a vacuum. Even if, for argument's sake, one accepts that Cisco did not market these products specifically for prohibited law enforcement purposes, the company had ample reason to know that Chinese law enforcement agencies were engaging in Internet monitoring activities on a massive scale, and that the sale of these products and technologies could easily be misused to facilitate exactly the type of Internet monitoring and human rights abuses that U.S. laws and policies condemned. A number of highly reliable sources, including the U.S. Department of State in its annual Human Rights Country Reports on China, numerous international human rights organizations, and the media, have been making clear for many years what China was planning and doing with respect to the repressive monitoring of the Internet and electronic communications. Cisco was on full notice, and should have had no doubt about what these products and technologies were going to be used for. Indeed, Cisco's marketing material made clear that they fully realized the unlawful law enforcement purposes that attached to their exports. Turning a blind eye to reality and to the violation of U.S. law that was involved in these sales and exports was not a reasonable or lawful business practice.

Third, the Compliance Guide just issued by the Commerce Department's Bureau of Industry and Security makes clear that a company's obligations to monitor and comply with Export Administration Act requirements and prohibitions go beyond just determining whether the equipment that is the subject of a

proposed sale is listed among the categories and types of products whose exports are restricted. ***Especially*** where “dual use” types of equipment such as computers and electronic communications products are involved, a company must make a realistic assessment as to the end users and the end use that their products will be associated with. In Cisco’s case, the end users were law enforcement agencies in China, and the end use was ***represented and acknowledged by Cisco officials themselves*** as being associated with Internet surveillance activities specifically designed to identify and arrest dissidents. As such, Cisco’s actions constituted a *per se* violation of U.S. export control laws.

Just prior to the May 20, 2008 hearing before this subcommittee, an internal Cisco powerpoint presentation relating to a sales pitch to the Chinese government was leaked to the public, in which a Cisco employee took note of the Chinese government’s aim to “combat 'Falun Gong' evil religion and other hostilities” and suggested that purchase and use of their product would increase the capability of Chinese law enforcement agencies to monitor Internet use and to identify dissident users. This demonstrates undeniably that Cisco knew that the supposedly neutral or dual use products and technologies it sold and exported to Chinese authorities could easily be used for purposes prohibited by U.S. law, for the surveillance and monitoring of Internet and electronic communications for law enforcement purposes.

Mr. Chandler’s responses to questions posed during and after this hearing demonstrated Cisco’s cavalier attitude toward its critical role in enabling China to carry out internet-based acts of repression. While Mr. Chandler stated during the hearing that he was “appalled” and “very disappointed” to see such language included in the leaked document [p. 17 of May 20, 2008 hearing transcript], he did not deny that Cisco knew that one purpose of the Chinese Government’s Operation Golden Shield project of Internet monitoring was to combat Falun Gong and other religious and political dissidents. [p. 38-39] Moreover, in neither his oral statement nor his written responses was he able to identify any specific ways in which Cisco sought to ensure that China could not use its products in such a way as to undermine human rights. All he could muster was a reference to a very general policy requiring that employees “treat others equally and with respect and dignity.” [e.g., pp. 21, 36-37] Similarly, Chandler was unable to indicate that Cisco informs government clients, in writing or otherwise, that Cisco would not assist in efforts toward censorship and repression, nor was he willing to commit the company to doing so in the future. [e.g., pp. 22, 38] Finally, Chandler suggested that Cisco was too large, and conducted too much overseas business to properly monitor the behavior of all its foreign-based employees and affiliates with regard to any support they gave foreign governments in their acts of repression, as evidenced, for example, by Cisco’s powerpoint presentation for the Chinese authorities that promoted the sale of Cisco routers for the specific purpose of enhancing Internet monitoring activities. [e.g., p. 39]

As a result of information that has been unearthed by this Committee and by other sources, Cisco's unlawful and unethical sales to the Chinese authorities has been garnering substantial attention over the past few years. Shareholders are demanding through shareholder resolutions and proposals that the company take tangible action to end its involvement in internet-related human rights violations, and adopt institutional procedures and mechanisms to identify and prevent questionable sales that would have negative human rights impacts. For example, Boston Common Asset Management and RiskMetrics Group, representing over 24 million shares of Cisco Systems stock (NASDAQ: CSCO) totaling over \$580 million have submitted a number of shareholders' proposals over the years "to take concrete steps to mitigate human rights related risks that could ultimately stifle long-term demand for the networks it builds (Boston Common release of November 10, 2009 titled: "Investors Representing Over \$580 in Cisco Shares Are Urging Cisco to Respond to Human Rights Risks In Its Global Operations"). They requested more openness from Cisco in providing "additional information in its existing public documents on policies and practices related to doing business with governments that restrict certain human rights," and sought adoption of a policy to refrain from selling products that would aid in repressive actions by foreign governments. They noted that Cisco is "not immune" to risks to the company posed by sales that promote human rights abuses, and that "Cisco's responses to our concerns have been wholly inadequate," according to Adam Kanzer, Managing Director and General Counsel of Domini Social Investments, one of the sponsors of the proposals.

Shareholders have good cause to be concerned about Cisco's China sales, not only from a legal and human rights standpoint but also from a fiscal standpoint. The illegal and imprudent actions of Cisco's leadership in selling products to the Chinese authorities for the use in law enforcement activities, in contravention of the Tiananmen Square Provisions of the Export Control Act, expose the company to a host of negative consequences, all of which jeopardize the company's financial position. The Department of Commerce would be fully justified in bringing both criminal and civil enforcement action against Cisco, potentially resulting in substantial fines and considerable negative publicity for the company. The May 2008 hearings of this Subcommittee focusing on Cisco's human rights violations, and these follow-up hearings today, are only the beginning of the negative public attention that will be coming Cisco's way unless they stop these unlawful and unthinking practices and develop a substantial company-wide policy and compliance mechanism to prevent these human rights abuses in the future. The mounting negative publicity focused on Cisco and its China sales worries shareholders, as it sheds doubt on the capability of the company's leaders to carry out their responsibilities in accordance with the law, and the appropriateness of actions that could cause their investments to decrease in value.

The newly issued BIS Compliance Guide sets out a very compelling explanation of the negative impacts on a company that may well be associated

with improper and unlawful exports of the type we are discussing involving Cisco and China. For example, page 122 of the Guide notes that companies “may be subject to criminal prosecution and/or administrative penalties,” and suggests that “Bad publicity alone can cost companies incalculable sums, in terms of future business, not to mention costs associated with lengthy and costly litigation, or administrative or criminal penalties.” The Guide makes clear that it is the company’s obligation to “be aware of suspicious circumstances and Red Flags that may be present in an export transaction,... [to] evaluate all of the information after inquiry and refrain from engaging in the transaction if the Red Flags cannot be resolved.” Cisco’s handling of its marketing and exports to China suggests it has not followed these recommended, acceptable good business practices.

What Congress and the U.S. Government Must Do

To this Subcommittee's great credit, in Part I of its hearing involving Cisco in May 2008, it asked Cisco a number of probing questions regarding the details of the company's sales to the Chinese authorities and the ways in which the company ensures that while selling products to repressive regimes it is not complicit in human rights violations carried out by those regimes. Siimilar questions were directed at Cisco in the letters sent by this Committee to various U.S. companies including Cisco notifying them of today’s hearings. Regrettably Cisco failed to respond in any meaningful way, and therefore these questions remain unanswered. Going forward, Cisco should be required, at a minimum, to provide this Subcommittee with specific information regarding a number of important topics:

First, in Congressional hearings Cisco has cited to its own company’s Code of Conduct as serving to ensure that its employees do not customize Cisco products in such as way as to undermine human rights, or market its services to government authorities in China or any other nation on the basis of their usefulness in detecting, monitoring, or censoring political dissent or expression. Cisco should be required to provide the subcommittee with a copy of its Code of Conduct and any other relevant Cisco documents, particularly those developed after the 2008 subcommittee hearing, highlighting the portions that are relevant to the sale of its products to governments that are known to use them for law enforcement purposes. Cisco also should provide details of all cases where the Code of Conduct and any other relevant standards along these lines have been applied in the past in situations in which sales to China and other repressive regimes have been considered, or have taken place.

Second, Cisco should be required to provide detailed information on any mechanism that it has in place, or is considering, to monitor and assure compliance with its own Code of Conduct, and with U.S. export and human rights laws. Does Cisco have a compliance officer to monitor these issues, or a compliance process in place to assess, in advance, the impacts of sales to countries that are known to use Cisco products for law enforcement and

repressive purposes? Did that officer or process pass judgment on the appropriateness of the decision to market or sell the products under discussion to Chinese law enforcement agencies?

Third, Cisco should specifically identify and describe each and every product and technology that it has exported to China, when these transfers occurred, whether export licenses were applied for, and what specific entities were the recipients and users of each of these products. Additionally, it should address whether the company conducted any sort of process to evaluate potential misuse of the product, or what entities would be the end users, consistent with, or at least along the lines of, the Guidelines on Compliance that BIS has just issued.

Fourth, how many law enforcement marketing shows in China, or involving Chinese law enforcement agencies, has Cisco attended since 2002? How many sales to Chinese law enforcement agencies have taken place since 2002, and what was the nature of the products or technologies sold? What entities were the buyers and recipients of these products?

Without this information – which can only be provided by Cisco – there is no real way to assess the extent to which U.S. export laws have been broken and whether Cisco conducted the appropriate and necessary steps to make sound and lawful business judgments regarding proposed exports when the products and technologies were being marketed and sold to China.

In addition, Congress also must pay much more attention to how and whether the Department of Commerce's Bureau of Industry and Security is doing an adequate job of carrying out its responsibility to monitor and assure compliance with various provisions of the Export Administration Act that have been given short shrift in the past, including the Tiananmen Square human rights prohibitions.

Finally, Congress must not only pass the existing provisions of the proposed Global Online Freedom Act, but must give careful consideration to whether the present draft of that Bill goes far enough in dealing with the emerging issues of U.S. company involvement in major human rights abuses, and cyber attacks by repressive foreign governments and their agents.

Our nation's national security interests, as well as our firm commitment to human rights, demand that we hold our corporate entities accountable in this area, and make sure that U.S. companies do not contribute to or facilitate the repressive and intrusive actions by foreign governments and their agents involving Internet use and electronic communications.