"China's Information Control Practices and Implications for the U.S." U.S.-China Economic & Security Review Commission June 30, 2010

Testimony of Rep. Chris Smith Ranking Member, House Subcommittee on Africa and Global Health House Ranking Member, Congressional-Executive Commission on China House Ranking Member, Commission on Security and Cooperation in Europe

Thank you, Mr. Chairman and members of the U.S.-China Economic and Security Review Commission, for this opportunity to testify on the Chinese government's information control practices.

I'd like to concentrate my testimony on the control of the Internet, since the Chinese government, more than any other, has developed and deployed the methods and technologies that it and other governments use to transform the Internet into a tool for surveillance and censorship. In the world of Internet repression, "The Great Firewall of China" sets the standard for worst practices.

Reporters Without Borders documents that, in China alone, at least 72 people are imprisoned for Internet postings. But the Chinese government's injustice to these people, and their suffering, is only the tip of an enormous iceberg. The Chinese government subjects an uncountable number of people to Internet-related human rights violations, from Falun Gong practitioners tracked down through the Internet (and, once found, subject to unspeakable abuse), to Tibetans and Uyghurs denied all Internet access for extended periods, to democratic reformers intimidated and stifled, to religious believers unable to express their faith and communicate with each other freely. In the end, the victims of the Chinese government's information control practices include the entire Chinese people: denied access to information and ideas, denied their right to free expression, spied on by their own government, and self-censoring in an intentionally created atmosphere of fear. Even beyond this, the Chinese government's victims include many peoples in other countries, tyrannized over by governments with which the Chinese government shares its technologies and techniques of repression—there are solid reports that these include Cuba, Vietnam, Burma, Belarus, and Sri Lanka, and almost certainly there are other victim-countries.

The implications of this for the United States are grave. The Chinese government coerces U.S. IT companies doing business in China to participate in its Internet repression. This has been notorious since 2006, when I chaired an eight-hour hearing on *The Internet in China: A Tool for Freedom or Suppression?* The hearing responded to Yahoo!'s cooperation with Chinese Internet police's tracking down of journalist Shi Tao—who is still serving a 10-year prison term for disclosing state secrets, that is, e-mailing to the U.S. Chinese government orders not to report on the 15th anniversary of the Tiananmen massacre. Google, Yahoo!, Microsoft, Cisco, among others, testified at that hearing, which broke the ground on the issue of Internet freedom. At that hearing the world learned the extent to which some of America's most prestigious companies were cooperating with the Chinese government in gross human rights violations.

This has implications for all of us. U.S. companies and U.S. citizens are involved in the Chinese government's human rights violations, in denying people their freedom of expression rights, and

this can only degrade the standards of American business. If this isn't changed—and I believe our government has a responsibility to protect and promote freedom of expression—it will eventually affect the kind of country we live in. If we accept these business practices as "normal," we'll become desensitized, shrug our shoulders at violations of a basic right—freedom of expression—that has always been a hallmark of who we are as a people.

I also want to point out that the Chinese government's Internet repression threatens our own freedom in a more direct way. For many countries in Asia and Africa, China has become the new model. People throughout Asia and Africa admire China's economic growth, but their dictators also admire and are setting out to imitate the Chinese government's ability to combine growth with one-party control. And China is actively promoting its system among these governments, including its system of Internet repression. Since 2006 the technology of Internet repression has grown more sophisticated, and freedom of expression is in retreat. This is a long-term threat to our own freedoms.

Yet we have also learned some positive lessons since 2006. We have seen that many US IT companies really want to do the right thing. Google's transformation has been remarkable. Since 2006 I have been meeting with Google executives, and its statement in January that it is "no longer willing to continue censoring" results on its Chinese search engine, was remarkable and thrilling—certainly the hearts of millions of Chinese human rights activists and political and religious dissidents. Despite what some critics have said, Google's decision this week to stop automatically re-directing google.com.hk, does not diminish what the company has done. Google never promised to automatically redirect any searches, but said it would not continue censoring. Google has lived up to that.

But Google has not had the support from our government that it should, and I think most of us expect it will be pushed out by the Chinese government, though perhaps gradually. Google's difficulties in China make it clearer than ever that, however well-intentioned, American IT companies are not powerful enough to stand up to a repressive government like the Chinese.

The Global Online Freedom Act, the legislation I crafted in 2006 and re-introduced in this Congress, would give these IT companies the US-government back-up they need to negotiate with repressive governments like China's.

Let me describe the bill's key provisions. The bill would establish an Office of Global Internet Freedom in the State Department, which would annually designate "Internet restricting countries"—countries that substantially restrict Internet freedom relating to the peaceful expression of political, religious, or ideological opinion or belief. US IT companies would have to report to the State Department any requirement by a repressive government for filtering or censoring search terms—and the State Department would make the terms and parameters of filtering public knowledge, thus "naming and shaming" the repressive countries.

US IT companies would also have to store personally identifying information outside of Internetrestricting countries, so that the repressive governments wouldn't be able to get their hands on it to track dissidents. US IT companies would have to notify the Attorney General whenever they received a request for personally identifying information from a repressive country—and the Attorney General would have the authority to order the IT companies not to comply, if there was reason to believe the repressive government seeks the information for other than legitimate law-enforcement purposes.

In short: GOFA would give the IT companies the back-up of the U.S. government. If the Chinese or Iranian government tells them to filter a search term, they can point to the GOFA and say that US law doesn't permit it. If the government's Internet police intercept a human rights activist's e-mail, and demand the company turn over personally identifying information on the account, the company will notify the AG, who can then bring the weight of the US government into the matter.

GOFA has the distinction of being endorsed by Google as well as a long list of human rights groups—Reporters Without Borders, Amnesty International, Laogai Research Foundation, Human Rights Watch, Committee to Protect Journalists, International Campaign for Tibet, and others. In the last Congress it was passed by three committees.

The situation has grown too serious for Congress to settle for meaningless, softball legislation on this issue. Now we see that every time a repressive regime cracks down, Internet censoring, blocking, and surveillance is one of the most powerful weapons in its armory—that was the case when the Chinese government cracked down on largely peaceful protests in Tibet in 2008, when it cracked down in protesting Uyghurs in Xinjiang in 2009, and when the Iranian government cracked down on post-election protests this summer.

I ask the members of the commission, and everyone here today, to take a good look at this bill. Speaker Pelosi said it very well in January: "The Chinese government operates one of the most sophisticated operations in the world to control the Internet. It is essential that technology companies not assist in efforts that violate human rights or prohibit free exchange of ideas." It's time for meaningful action on this issue—one of the most burning human rights issues of the day.