Testimony of

Shiyu Zhou, Ph. D.

May 20, 2008

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

Hearing on Global Internet Freedom: Corporate Responsibility and the Rule of Law
May 20, 2008

Testimony by Shiyu Zhou, Ph.D.
Deputy Director, Global Internet Freedom Consortium

Mr. Chairman, members of the Committee, Ladies and Gentlemen. I would like to thank you for this opportunity to testify before you today on the topic of global Internet freedom and the Corporate Responsibility and the Rule of Law.

The lack of information freedom in closed societies is usually coupled with severe violations of human rights and it also puts the United States at risk. In Iran, Cuba and certain other totalitarian countries, information control is often used for manipulation and indoctrination and whipping up anti-US sentiment, as illustrated by the xenophobia fostered online in the People's Republic of China (PRC) following the Tibet crackdown and the Olympics Torch Relay. Violence begins with hate, and hate begins with distorted information.

Information control can also cost lives. When the PRC leadership chose to suppress news of the SARS outbreak in 2002, the virus spread far beyond China's borders to places like San Francisco, causing the death of at least several hundred victims and almost a global pandemic.

The Internet has become the greatest hope for global information freedom. It is a vast, fast, and inexpensive way to access information and to communicate and the number of Internet users worldwide has soared. By January of this year, the PRC had 210 million users and has since surpassed the US, and both Iran and Vietnam were at 18 million users and growing. While authorities in closed societies can easily shut down newspapers, block TV channels, jam short-wave radios, and ban books, the Internet is far more elusive. With the proper anti-censorship technologies, users in these societies can access uncensored information online freely and without fear of reprisal. Anti-censorship is sometimes called anti-blocking or anti-jamming and refers to technical means that protect users in closed societies from being monitored, blocked, or tracked.

For more and more users around the world, that proper anti-censorship technology means tools like FreeGate and UltraSurf -- created by the Global Internet Freedom Consortium (GIF), a small team of dedicated men and women, connected through their common practice of Falun Gong, who have come together to battle tens of thousands of Internet monitors and censors around the world to work for the cause of Internet freedom. I am proud to stand before you today on behalf of this illustrious group because I feel they are truly heroic. They have allowed millions of citizens inside repressive societies to experience the Internet as we in free societies experience it - being able to use Wikipedia to look up a new word or post a blog without having to look over their shoulders. The Consortium provides its products and support services to those citizens entirely free of charge.

The companies and organizations that make up the Consortium have maintained the world's largest anti-censorship operation since 2000. The focus was originally on the PRC as China's censorship measures on the Internet are by far the most sophisticated and extensive among all the closed societies. As more and more nations have followed China's lead, however, our experience has made us uniquely equipped to help advance Internet freedom around the

globe. Outside of China, the second largest segment of our user base is now in the Middle East: in Iran, Saudi Arabia, United Arab Emirates, and Syria.

Of the 43 countries identified as "Not Free" in Freedom House's Freedom of the Press 2008 Survey, GIF's anti-censorship systems have served users in the following 33 countries as of January 2008: Algeria, Angola, Azerbaijan, Belarus, Brunei, Burma, Cambodia, Cameroon, China, Congo, Cote d'Ivoire, Cuba, Egypt, Iran, Iraq, Kazakhstan, Laos, Libya, Maldives, Oman, Pakistan, Qatar, Russia, Rwanda, Saudi Arabia, Sudan, Syria, Tunisia, United Arab Emirates, Uzbekistan, Vietnam, and Zimbabwe.

Our five existing tools - UltraSurf, DynaWeb FreeGate, Garden, GPass, and FirePhoenix -- currently accommodate an estimated 95% of the total anti-censorship traffic in closed societies around the world, and are used DAILY by millions of users. These tools have been of benefit to US-based organizations such as Human Rights In China, the Chinese Democracy Party, Voice of America, and Radio Free Asia -- and even companies like Google and Yahoo since we bring the uncensored version of their services into closed societies like China.

As of January 2008, the Top Five censoring countries with the most average daily hits to our anti-censorship systems are (hits per day):

(a) China: 194.4 million
(b) Iran: 74.8 million
(c) Saudi Arabia: 8.4 million
(d) UAE: 8 million
(e) Syria: 2.8 million

Clearly, besides China, a significant portion of the user base is from the Middle East.

We have witnessed first-hand the effectiveness of anti-censorship technologies in improving information freedom for people in closed societies. During the democratic movement in Burma in late August 2007, our anti-censorship portals were receiving over 120,000 average hits from IP addresses originating inside Burma every day; a three-fold increase from less than 40,000 prior. That number has since more than doubled in the wake of the cyclone.

After the protests broke out in Tibet on March 10 of this year, there was a four-fold increase in the number of daily hits to our anti-censorship portals from Tibet, from the daily average of 120,000 before March 10 to about 480,000 after March 10. The daily number of hits reached more than 800,000 on March 16. The measures Chinese authorities have taken to clamp down on information going in and out of Tibet are severe. The Consortium's anti-censorship tools are now one of the Tibetans' few remaining links to the outside world.

A particularly insidious aspect to information control is that it allows a repressive government to spoon feed the populace with whatever false information it chooses. In closed societies such as China and Iran, censorship is used by the leadership to save face, deflect criticism, and turn domestic discontent against external enemies both real and imagined. A few carefully edited TV news segments, a few doctored articles in the newspapers, a few carefully placed key words to dehumanize the target, and the result is a very large and very hostile population. The US would do well to heed the very real threat this poses to our national security.

Internet freedom is one of the most effective ways to allow the US to win the hearts of the people in closed societies, and its young people in particular, and to help move the world in more benign and realistic directions. Anti-censorship technology can allow the people in closed societies to be better informed and to be less subject to manipulation by an unscrupulous leadership. Winning people over to a more open and free system via the Internet could very well be a way to avoid damage and loss of life in future conflicts. It is no exaggeration to say that an online information battle, if fought well, could ultimately help to prevent a real war.

It is thus not surprising that China maintains an Internet "firewall" bureaucracy of over 30,000 officials and that, as reported by the State Department/Foreign Operations Appropriations Committees, Chinese President Hu Jintao has spoken of a crisis involving "the stability of the socialist state" that will only be cured if the Internet can be "purified."

In the on-going struggle between the censors and anti-censorship efforts, it is crucially important to stay ahead of the game. Repressive regimes have been spending enormous sums on developing censorship tools in recent years. We should also be aware that China's military is actively developing sophisticated ways to wage digital warfare against America. For years, Chinese authorities have indoctrinated "patriotic hackers" to infiltrate and take down US government computer systems. Just recently, these hackers were instigated to attack the CNN website en masse. If the US does not maintain its current lead in anti-censorship technologies over censors now, there could be a much higher price to pay down the road.

Our statistical data show that currently Chinese elites are among the most avid users of our anti-censorship services, for they want to know what is happening in the world that their government does not provide them. It has been transforming the Chinese society in a peaceful but powerful way that must not be underestimated. Once a critical mass, 10 percent we believe, of the 230 million Internet users in China get to know the existence of our anti-censorship tools and, especially, gain a positive experience of using them, the avalanche effect of such a development will in our view lead to the fall of the Beijing censorship Wall and, consequently, to the fall of other Walls in the world's other closed societies. Imagine, then, the possibilities of the Pope being able to conduct an interactive worship service with millions of House Church Chinese Catholics, or Members of this Committee being able to conduct seminars in democracy with tens of thousands of Iranian students -- all without fear of detection or arrest using our scaled-up services.

The battle of Internet freedom is now boiling down to the battle of resources. It is our belief that $50 million - enough to allow GIF programs to scale up their operations through purchasing equipment and expanding network capacity - will be enough for us to reach the critical mass of 10 percent of the 230 million Internet users in China. Importantly, the time for doing so is this coming year, given the current political dynamic in China and the upcoming Olympics. We hope and trust the Senate and the Congress will grasp what we believe to be a historic opportunity.

Only when the US shows more determination to keep the Internet open than the closed societies are showing to seal it off, can there be the hope of information freedom and democracy for the citizens in all closed societies, and a more peaceful tomorrow for mankind.

We would like to thank Senator Leahy, Senator McConnell, Senator Gregg, Congresswoman Lowey, Congresswoman Ros-Lehtinen, Congressman Wolf, Congressman Berman, and other members of Congress, and Ambassador Mark Palmer of Freedom House, Michael Horowitz of Hudson Institute, former Director of NTIA Clay Whitehead, and Human Rights Watch DC Office Head Tom Malinowski, for the support they have provided my colleagues. In particular, we thank Senator Leahy, Senator McConnell, Senator Gregg, Congresswoman Lowey, and Congressman Wolf, for the Internet freedom initiative in the fiscal year 2008 Foreign Operations Appropriations Bill which set up a competition for a $15 million grant for "field-tested" Internet technology programs and protocols that, in the words of the appropriation legislation, "have the capacity to support large numbers of users simultaneously in a hostile internet environment."

Below is a more detailed description of the current state of Internet censorship around the world, how people have benefited from the services we've been providing, and how our services might be expanded to successfully tear down Firewalls in closed societies around the world.

The State of Internet Censorship

A number of countries actively censor the Internet, including Iran, the People's Republic of China, Burma, Saudi Arabia, and Vietnam. Since China's censorship measures on the Internet are by far the most sophisticated and extensive and are emulated by many other nations, the state of Internet censorship in China illustrates well the nature of the problem in other closed societies.

Since 1999, we have seen China's Internet censorship capability evolve from rudimentary measures to systematic and highly advanced technological deployments. Those of us who have worked for the world's top technology companies can tell that the capability and sophistication of the Chinese government's censorship technology is at such a level that they are using the most top-of-the-line, cutting-edge products.

Today there are three mechanisms at work on the Great Firewall. One is Internet Protocol Address blocking, or IP address blocking. An IP address on the web is like a phone number on a telephone network. IP address blocking is simply denying your visit to overseas websites with certain IP addresses. The websites targeted by the censors are mostly about Falun Gong, the Tiananmen Square massacre, Tibet, Taiwan, human rights, etc.

The second mechanism is called content filtering. Chinese authorities have built powerful net machinery to sniff all the net traffic going through the Great Firewall in either direction. Once they detect a keyword in the traffic, they will simply cut off that particular traffic flow. The user ends up staring at a blank screen as though he has suddenly lost his Internet connection. This method indiscriminately blocks access to any site that happens to have one of the keywords included on the long official list.

The third mechanism is the most malicious - we call it Domain Name Redirect. This method can be likened to publishing a phone book with the number of the people you dislike changed to other numbers so no one will ever be able to reach these people. Another analogy would be changing all the street signs so no one knows where they are actually going. This is a flagrant violation of international Internet conventions and standards on a national-scale, but apparently the censors do not feel any obligation to play by the rules when they want to control information.

Besides the technological aspect, there is a whole other dimension to censorship on the Net. We call it the "human flesh Great Firewall." At the top is an army of tens of thousands of net police patrolling the web space in China. Down below are countless website administrators who are forced to sift through the blogs, forums, and bulletin boards they are managing to delete any posts deemed "sensitive" according to certain arbitrary rules. In addition, Internet service providers (ISPs) are told to keep an eye on the sites they are hosting and be ready to shut down the sites that cross another arbitrary line drawn by the state. Internet content providers such as search engines and portal sites also devote significant time and effort in preemptive self-censorship.

Demand and Impact of Anti-censorship Services

Since the early days of the censorship, we have been providing censorship-circumvention service to users living in oppressive regimes. We started as a few independent and scattered groups, including Dynamic Internet Technology, Inc. (DIT), UltraReach Internet Corporation, Garden Networks for Freedom of Information Inc., World's Gate, Inc., and Global Information Freedom, Inc. Each group had a different technical approach.

Our services were originally targeted towards and promoted to Internet users in China, but over time we have also attracted a large number of users from other closed societies, such as Iran, Burma, and Saudi Arabia.

In 2006, these groups formed a consortium, Global Information Freedom Consortium to pool their experience, infrastructure, resources, and technological talents together. The purpose was to provide better service to users and beat censorship more effectively, especially when each of the groups had limited resources.

Our anti-censorship services were developed and evolved in response to two major user demands: to surf the web freely and securely and to post information on the websites inside China without exposing the identity and origin of the connection. Our services have three major facets:

1. Anti-censorship tools: These are a variety of software tools we provide to users to defeat blocking, monitoring and tracing of their online information and activities. When a user in China fires up our system, the bits and bytes flowing in and out of his/her computer are scrambled, so the Great Firewall cannot see any patterns in the traffic and therefore has no idea if it detects something suspicious or not. Additionally, our tools are highly dynamic and know where the cracks in the Great Firewall are. The tool changes its network connection from time to time to avoid becoming a sitting duck.

Currently we have five major tools from our coalition to cater to our users' demands, including DIT's FreeGate, UltraReach's UltraSurf, Garden Networks' Garden, and World's Gate's GPass and FirePhoenix. They have different features and technical strengths and they are also constantly evolving in response to the ever-changing censorship technologies.

The variety of our tools provides our users with a real edge. They have reported that with such a selection, they are almost unstoppable. Whenever one of our tools is jammed by the censors, a user can switch to another tool to either get back online or download a newer version of the jammed one. Such a complementary nature seems to greatly enhance the users' confidence in our offerings.

2. Infrastructure: Once a user launches one of our tools, information is relayed to a network we have built in free countries, mostly in the U.S. This network is like an Underground Railroad in cyberspace, but much more dynamic. The capacity of this infrastructure directly impacts the number of users we can support.

This network also provides extra services. For example, World's Gate provides low-cost web-hosting services to users in closed societies so they can enjoy freedom of expression by establishing forums, discussion groups, etc. on our network in addition to the native support of censorship-resistance.

3. Promotion and user support: We have found it is critical to perform user outreach, because the news about the availability of our services is itself blocked. Therefore we have to actively spread the word via the Internet using emails, instant messages, forum posts, and traditional means such as long-distance telephone calls and postal mail. Once the user base reaches a critical mass, it becomes much easier because the news can be spread through word-of-mouth.

Timely technical support for users is a must for a successful anti-censorship system. Our five systems (FreeGate, UltraSurf, Garden, GPass and FirePhoenix) are now sharing a unified technical support platform, www.qxbbs.org, in which each system has its own user forum. It is a place where users can share their experiences and developers can provide technical support. For example, there are more than 20,000 posts on DynaWeb's support forum with information ranging from technical tips to compliments from users to reports from China of new blocking test results. This operational area also includes internationalization, i.e., translation of user interface, documentation and instructions into users' native languages.

Currently the Consortium is running the largest anti-censorship operation serving 95% of the circumvention traffic from about 2 million users.

Our services are not limited to Chinese users. Within two days in January, 2008, we witnessed on our system users from 33 out of the 43 countries identified as "Not Free" by Freedom House's Freedom of the Press 2008 Survey, GPass has become a favorite with Iranians ever since it released a Farsi (Persian) version.

Our services have also benefited US-based organizations such as HRIC, the Chinese Democracy Party, VOA, and RFA.

Our Challenges

As a grassroots organization, we feel we have been fighting against a Goliath in cyberspace alone. Challenges we have been facing include:

1. Censors using high-tech equipment with ever-increasing performance for Internet snooping and control. The intelligence of our adversary, as well as our own system, learns and evolves with time and with experience, and with high-end machinery.

Although we have not physically seen the machines in the server room of those in charge of maintaining the Chinese Firewall, the advanced capabilities indicate they constantly upgrade their hardware with top-of-the-line items on the market.

2. Resource limitations. So far our endeavor has been sustained mostly by volunteers. On the one hand, more and more users are eager to get on our Underground Railroad; on the other hand, we have limited bandwidth, hardware, manpower, and time to expand and satisfy their needs.

I believe we have the most advanced anti-censorship technologies around. That is why we are ahead of the game most of the time, and why we have been able to support an ever-increasing user base. But technology is not the only determining factor. The game is now boiling down to a battle of resources. Besides the hardware of the Great Firewall, the censors have also assembled an army of tens of thousands of net police to serve as a human flesh Great Firewall. That is a challenge for us because our current resources make it difficult if not near-impossible to match that kind of manpower. On the other hand, our experience indicates every penny we invest in our offense will force the censors to burn a dollar or more in defense. So every penny counts a lot in our effort.

3. Attacks from all directions. The Chinese Communist Party (CCP) has no interest in playing a fair cat-and-mouse game on the Internet. It constantly launches cyber attacks on our infrastructure and our people. Attempts to hack our websites are non-stop, emails impersonating our own people with virus attachments are abundant, harassing phone calls are not rare events. It even resorted to physical violence on U.S. soil when other measures failed: Armed Asian men broke into the home of the president of our organization, Yuan Li, in Atlanta, brutally beat him and stole his computers while leaving other valuables intact. We have reason to believe the CCP was behind the attacks.

As a side note, we would also like to point out that it seems the CCP has been using our systems as practice targets before it launches attacks against US and other countries' government networks. The tactics used in these attacks share much similarity with what we have seen.

Besides the direct attacks, the Chinese regime has also forced anti-virus companies in China to identify our software tools as viruses to discourage users from adopting the software. Surprisingly, anti-virus companies in the US such as Symantec and Norton do not seem to want to be left behind as their anti-virus software also indiscriminately labels some of our tools as viruses. Our written clarification with them has fallen on deaf ears.
Despite all the difficulties, we have not wavered from our mission. Many of us have witnessed first-hand the Communists' brainwashing, hatred induction, and indoctrination, and we treasure the information freedom outside the Great Firewall. However, the people still confined within the Great Firewall need much more help. We urge government agencies, NGOs, and corporations to step in and contribute to these efforts.
For democratic governments, many actions can be taken to bring the anti-censorship endeavor to the next level. For example:

Provide resources to these efforts. This is the most effective support. Since anti-censorship technologies have matured and have been field-tested, most resources are now devoted to the operation of these systems instead of to research and development. The impact of such support would be immediately visible. The government should measure its achievements by not only the number of political prisoners released, but also the number of users who are enabled and empowered to access information freely.
Limit technology exports to repressive regimes. Evidence shows that the advanced Internet filtering technologies used in the Chinese Great Firewall are provided by Western companies. Democratic nations should impose restrictions on such exports as they can be exploited for future enhancements of the Firewall.

Establish a funding vehicle to rally financial and resource support from other organizations and corporations. In particular, those multi-national technology companies such as Yahoo! and Google that have said it is not "convenient" for them to provide an uncensored web to users in China could contribute to our efforts and we would be happy to step in.

The United States funded the creation of Internet a few decades ago. Now the Internet is used in repressive regimes as a powerful tool to suppress freedom and is being morphed into a dark weapon for cyber war targeting the US and other free nations. Please allow us to submit our humble opinion that defending the transparency and freedom of the Internet is of critical national interest and we believe the US government has a responsibility to play a much more active role in this endeavor.

****

The Roles of US Companies in China's Internet Censorship

There is unfortunately strong indication that companies in free societies such as Cisco may have involved in assisting the Chinese security services to monitor and censor the Internet, and persecute and prosecute Chinese citizens who just want to use Internet to access uncensored information and/or express their own views freely and peacefully.

In a 2002 Cisco (China) PowerPoint presentation entitled "An Overview on [China's] Public Security Industry," now in our possession, a Cisco (China) official in the Government Business Department listed the "Golden Shield Project" - the host project of China's Great Firewall - as one of Cisco's major target customers. One of the main objectives in that Project, defined in the Cisco document as the "Monitoring and Control System for Public Internet Information Security," was to "combat the 'Falun Gong' evil cult."

We must take note that the two words of evil cult, the rhetoric of the Chinese Communist Party to persecute Falun Gong, are not even quotation-marked in the presentation. The view taken of my fellow-practitioners in the PowerPoint document raises obvious and profound concerns about Cisco's culpability in an Internet monitoring and censorship regime that has diminished freedom, added to the power of a powerful dictatorship and, in pursuit of those goals, caused the arrest and frequent murder of innocents at the hands of China's Firewall bureaucracy.

In the following PowerPoint page headed "Cisco Opportunity [on the Golden Shield Project]," Cisco listed the following four areas of potential assistance to China/business opportunities:

"* High start-point planning;
"* High standard construction;
"* Technical training; and
"* Security and operation maintenance."

The above areas of potential assistance appear to flatly rebut Cisco's repeated and self-serving claims that it has merely sold routers and other equipment to China's security services and has not in any way assisted or participated in the Internet censorship and monitoring activities of those security services.

In the battle between our Consortium and the totalitarian Chinese authorities, it appears that Cisco is selling router equipment to the Chinese police authorities by offering censorship training and other supports. Our research shows that the main Internet censorship of China involves IP blocking, content filtering and connection reset, and DNS hijacking, and they are all done at the national gateway level. The infrastructure of China's Great Firewall shown by our research coincides with the layouts in Cisco (China)'s PowerPoint document.

We must appeal to these US corporations to reconsider what they are doing. Every time our anti-censorship tools are attacked using their technology, they are taking the side of the totalitarian authorities against Chinese people seeking some of the most basic of human rights. They are jeopardizing U.S. national security interests by directly compromising the safety of millions of Internet users in closed societies around the world. This is no longer just a virtual game, and it is certainly no longer just about dollars and cents. Real lives are at stake. Just ask Yahoo! how Mr. Shi Tao is faring as a prisoner of conscience facing several more years in his prison sentence for sending an email.

Our Consortium has been able to stay ahead of the censorship game by developing new software and new technology, but each battle has been grueling and certainly taps into our already scarce resources. Sometimes we feel like a little David fighting a constant battle with a monolithic Goliath out in cyberspace. It has been a lonely battle thus far and we are tired of having to fight our fellow American companies.

We intend to further investigate the history, use and meaning of the PowerPoint document, and to investigate all forms of assistance that Cisco officials may have given to China's Firewall and police bureaucracies in the latter's determined efforts suppress free Internet use and to brutally punish users and facilitators of uncensored Internet access. We call on Cisco to determine, on the basis of a thorough and searching investigation, the manner and extent to which the PowerPoint document was used and circulated within Cisco (China) and the extent to which the document's views were shared within Cisco (China). (We would like to know what the reaction of Cisco (China) officials was to the document's characterization of Falun Gong as evil.) We call on Cisco officials to acknowledge, immediately, once and for all and, at a minimum, that they can no longer assure Congress that Cisco (China) is and

has been a merely passive seller of routers and other equipment to China's security services, and we further call on senior Cisco management to acknowledge that they can no longer assure Congress that Cisco (China) has not been and is not now an accomplice and partner in China's Internet repression and, whether directly or indirectly, its infamous "610 Office" persecution of Falun Gong practitioners in China.

A cloud of suspicion now hangs over Cisco, which self-serving assertions of innocence can no longer dispel. Nothing but the most thorough and independent investigation, which we hope will be closely monitored by this Committee, will remove the concern that, in its efforts to sell routers and other equipment to China's security police, Cisco (China) officials were complicit in the persecution of those who bravely work to end China's efforts to monopolize the free flow of information to, from and between its people.

We conclude by noting another form of censorship, namely, self-censorship by content providers or websites operators. International companies doing business in censorship countries, such as China, restrict themselves and provide tailored content to users in these regimes. A prime example is Google's Chinese version, which provides drastically different search results for queries originating in China from its versions in other locations. As a U.S. company that appears not to be aligned with the repressive forces in China, Google's collusion and collaboration with the repressive weapons of censorship make the efforts of those seeking to expose the Chinese people to the market place of ideas all the more difficult. Unfortunately, there exist no effective technical measures to overcome this form of censorship.

So far the public have learned about Google's self-censorship mainly through media reports and rights organizations. Google itself has been silent about it. We believe that all Google users and shareholders deserve to know exactly what Google does to the 230 million Chinese Internet users. We therefore created the "Google Search Review" service, http://gg.edoors.com, that compares search results from google.com and google.cn.

We would like to offer the code to this Committee and to Google, and we respectfully request Google to host this service on their servers, and announce it to the public.