Written Statement of:

Robert Faris
Research Director
Berkman Center for Internet & Society
Harvard University

September 28, 2009

Distinguished members of the committee:

I would like to start by expressing my appreciation to the U.S.-China Economic and Security Review Commission for the opportunity to speak today about these important issues. The Internet has emerged as an important venue for economic, social and political activity. Realizing the potential of the Internet for improving the lives of citizens around the globe relies upon protecting freedom of expression and privacy online. Government suppression of online speech continues unabated in China and the cooperation of technology companies is a critical element in the implementation of government content control mechanisms. Congressional engagement with these issues can play a vital and constructive role in the examination of the issues and search for solutions.

I am the Research Director at the Berkman Center for Internet & Society at Harvard University. A principal focus of my work there is the study of the influence of Internet-mediated communication, such as new media, on political processes, governance and democracy. I am also a member of a team of researchers at the OpenNet Initiative (ONI), a collaboration of four universities that examines Internet filtering, content regulation and surveillance around the world. I have also been a participant in the Berkman Center's work with technology companies, non-profits, socially-responsible investors and other academic institutions in the formation of the Global Network Initiative (GNI).

The Internet in China and the Role of Content Regulation

With well over 300 million people online, China is now the country with the largest number of Internet users in the world. Internet-mediated communication occupies a key role in the economic, social and political life of the country, and continues to grow in importance by the day.

For a country that has traditionally maintained tight control over its media, the explosion of Internet use in China has presented government authorities with a formidable challenge: restricting online speech without impeding the potential of the Internet for economic, cultural, social, political and educational advancement. As more Chinese

users take to the Internet, there has been a tremendous increase in the use of social media and government content control mechanisms have similarly expanded in their reach.

The OpenNet Initiative has been studying and reporting on China's filtering mechanisms and content regulatory mechanisms for more than six years. Several reports available at www.opennet.net/country/china track the evolution of Chinese Internet restrictions and compare China's strategies to those of other countries around the world.

China employs an Internet content control system that is unparalleled in its reach and sophistication. At the core is a technical filtering system—often referred to as the great firewall of China—that blocks Web pages at several key points of control in the Chinese Internet, including international gateways and major ISPs. This filtering system is based on an extensive list of web sites compiled by the government that are targeted for blocking. This list is regularly updated to keep pace with political events and the introduction of new web sites. The web sites that are blocked span a wide range of content, including political, religious and social topics. Among other issues, web sites that include discussion of Taiwanese and Tibetan independence, the Tiananmen Square protests and the Falun Gong religious group are blocked extensively. The technical filtering system also includes keyword blocking that will sever Internet connection when a banned word is encountered in a web page address or search query. This keyword blocking system is unique to China.

In addition to the core technical filtering system, China employs a variety of control systems to limit the publishing of and access to sensitive information. Search engines are required to block the results of search queries, following broadly the same parameters used to block web sites. The extent of search engine result filtering is also unique to China. In both search result filtering and web site blocking, the strategy relies upon identifying specific Internet sites that produce objectionable content.

The rise of participatory media has complicated efforts to police online speech. The vast number of contributions from users distributed throughout China and other Chinese speakers from the globe means that blocking web pages is no longer enough, unless entire social media sites are rendered inaccessible. The political cost of such broad blocking would be considerable given the substantial comingling of political speech with otherwise innocuous speech on these platforms.

To address the issues that arise from social media, the government has had to explore different points of control and enlisted the help of content hosting providers such as blogging hosts and video hosting sites to police their own services. The government also reportedly employs Internet monitors to participate in online chat rooms and steer discussions away from sensitive topics. These content control mechanisms are backed by Internet laws that are as vague as they are expansive, providing a legal basis for pursuing Internet users who post content that crosses the fuzzy boundaries of acceptable speech in China.

The Chinese content control system combines these technical and legal, formal and informal controls at several different levels in the network which, in total, comprise the world's most comprehensive online content control system. The overall effectiveness of the system is difficult to assess as the key to its success is contingent upon the level of self-censorship that results from the combination of technical and soft controls. A sophisticated Internet surveillance system provides both a means to pursue offenders as well as a means of reinforcing the incentives for self-censorship.

Internet traffic patterns and the market structure of Chinese Internet services also contribute substantially to the information control apparatus. Stemming in part from the size of its Internet market, domestically run social media sites capture a large share of Chinese Internet traffic. The presence and popularity of domestically run Internet services expands the reach of government-mandated censorship efforts; Chinese regulators are able to readily enlist the assistance of these domestically run services to enable intensive monitoring of social media sites that wouldn't be otherwise impossible. The involvement of participatory media sites and online service providers in controlling Internet speech in China is unmatched globally.

The Chinese Internet filtering system is also notable for its lack of transparency and accountability. In many countries that filter the Internet, a block page is displayed to clearly signal to a user that they are being blocked. Users in China are not notified when web sites are blocked.

The Introduction of Green Dam

In May 2009, the Chinese government issued a directive that would require the installation of filtering software on new computers sold in the country. This marked a new and substantially different approach to Internet content control. The Green Dam Youth Escort software would increase the reach of Internet censorship to the edges of the network, adding a powerful control mechanism to the existing filtering and content control system.

The stated purpose of this software was to protect children from harmful Internet content. The software relies on lists of banned web sites and keywords analogous to those used by the centralized filtering system. The OpenNet Initiative carried out a rapid evaluation of the Green Dam software and found that the filtering options include blocking of political and religious content, which would constitute a much broader interpretation of content harmful to minors than we are normally accustomed. Moreover, the update features on the software can change the configuration and options of the software, such that the software could be modified for any number of purposes, including surveillance of individual computer use.

I have no insights into the true motives for introducing this software mandate. However, given the wide potential applicability of this software, the original intent of the policy is not as consequential as future decisions regarding its use would have been.

A key difference with filtering at the user level is that the processing power of the user's computer can be harnessed, allowing real-time content analysis. The Green Dam software can monitor the content of web pages as they are loading and close the user's browser when objectionable content is found. In testing the software, we also observed the software closing other applications without warning, including word processing software and spreadsheet programs. Chinese technologists who evaluated the software came to the same conclusions.

We were very critical of this directive for several reasons. As a policy decision, requiring the installation of a specific software product is not conducive for producing good software. Other researchers found significant security flaws in the software that would leave users vulnerable to hackers. I support the ability of parents to restrict the Internet uses of their children; offering software designed to give control to parents is a legitimate means towards this end. However, requiring households to have specific software installed is a very different proposition and one which I believe shifts far too much of this control into government hands.

While computer manufacturers scrambled to understand the implications of this mandate, significant opposition to the implementation of this software mandate emerged within China. The directive has since been softened and the software is no longer required for new computers sold in China. I applaud this decision. To me, this indicates that the government can be responsive to the input of computer users and technical experts and that public education, awareness and lobbying efforts can be influential.

I have no insight into the future direction of this type of policy mandate in China. The reintroduction of similar plans in China that would require the installation of software would undoubtedly be greeted with intense criticism and the same stiff opposition that emerged in this case. If the intent is to help parents protect their children from Internet content that parents deem harmful to the well-being their children, then facilitating the market for private sector software products would offer parents superior options for protecting their children.

The Dilemma for Technology Companies

The large and increasingly affluent population of Internet users in China constitutes an important market opportunity for ICT companies. Yet technology companies doing business in China face a conundrum. Internet firms that wish to compete significantly in the Chinese technology market are called upon to help with Internet content controls, just as domestic companies have been required to do. These companies inevitably face the prospect of requests for censorship and user information. Choosing how and when to comply with these requests is fraught with risks.

Acquiescing to the demands of the Chinese government without taking into account and defending the human rights of their users will come at a considerable cost at home, including negative publicity and pressure from the market, government and shareholders and scrutiny from human rights groups and other stakeholders. On the other hand,

refusing to cooperate with Chinese authorities could result in a company losing its operating license or putting their employees in China at risk of legal action. Chinese regulators may also block access for Chinese Internet users to the sites of companies that are not sufficiently cooperative, effectively putting them out of business for the duration of the block. Technology companies face a difficult set of decisions with significant risks on both sides of the equation.

The very notion of opposing the demands of Chinese regulators assumes that technology companies are able to properly sort what we would define to be legitimate law enforcement requests from illegitimate requests. In many cases, technology companies will not have sufficient information to make a definitive determination over the merits of a given request. Failing to comply with legitimate criminal investigations would have severe ethical and legal implications as well as damaging the reputation of the company and relationships with local governments. There is no simple solution to this tension as long as Chinese and US standards over legitimate censorship and law enforcement requests differ.

When considering the role of US companies in censorship and surveillance, it is important to distinguish between the business practices and products of different types of technology companies engaged in overseas markets. The experiences of Google, Microsoft and Yahoo! in China are well-known to the commission and have been documented in detail by the OpenNet Initiative and other research and advocacy organizations. However, as described above, the wide range of controls employed by the Chinese government implicates a broader range of ICT companies. Hardware providers may produce technology specifically designed to assist in censorship and surveillance, or dual-use technologies that provide other network functionality but that can be applied also to content control and user monitoring. Similarly, software providers produce products that are specifically designed to filter the Internet.

The activities of online service providers have been subject to more scrutiny as their actions are more easily observed and documented. This scrutiny serves a useful function and should continue. It is important to note, however, that the core competitive edge for these companies is providing their users with timely access to a full-range of online information and protecting their personal data from third-party intrusion. The incentives that these online service providers face are therefore broadly consistent with the promotion of freedom of expression and privacy online, veering away only to the extent that they are compelled to comply with regulatory mandates.

We know considerably less about the role of hardware and software providers. There have been allegations that US hardware makers have played a significant role in the development of China's filtering and surveillance systems. Better understanding the nature and impact of these business interactions in China should be a priority. The actions of these companies should be the subject of public scrutiny as well.

Promoting Constructive Engagement

I firmly believe that constructive engagement in the Chinese market is the best approach towards promoting freedom of speech and privacy online, despite the numerous thorny challenges that lie ahead. Even in the face of considerable Internet restrictions, the services offered via the Internet are bringing about noticeable changes in the social, cultural and economic life of China and contributing to greater openness. Only through continued commercial involvement can US firms play a constructive role in the development to the ICT sector in China. Many ICT firms have shown a commitment to push for greater transparency and accountability and through their ongoing engagement can help to solidify within China the benefits of increased access to information on the Internet. Defending the actions and rights of US technology firms working in China also offers a critical platform and focus for inter-government dialogue.

The alternatives to ongoing engagement are poor. Withdrawing from the Chinese market is unlikely to have any positive impact on the human rights situation there while souring the bilateral relationship. Abandoning this market would in all likelihood leave the commercial market to companies with a lower commitment to human rights. Given the availability of domestic alternatives, it would be a mistake to presume that China would miss western technology companies too much to let them go.

Yet, the road towards productive and constructive engagement is not clear. Ultimately, the decisions of Chinese regulators are of much greater consequence than any decisions taken outside the country.

In this context, a flexible approach to the issue is essential, combining soft measures, sustained dialogue, expanded transparency and diplomacy. Collective action—involving stakeholders from government, academia, business and non-profits—is a far better response than codifying measures that may prove to be counter-productive in this rapidly changing and complex environment. Placing legal restrictions on the actions of technology companies working in China may force them into an untenable legal situation in China and may unnecessarily force their withdrawal.

Where technology companies demonstrate a commitment towards protecting user rights, we would do better to provide them support in occupying a productive place in Chinese technology markets rather than placing impediments to their action. A collective, adaptive approach to these challenges appears to be the most productive response.

The Global Network Initiative

After more than three years of collective effort, negotiation and dialogue, the Global Network Initiative is showing substantial promise as a forum for evaluating and responding to the difficult challenges of working in countries such as China. This multi-stakeholder initiative, which includes representatives of industry, socially-responsible investors, non-profits and academic institutions, launched publicly in October 2008.

One of the key factors that will determine the success of the GNI is the effectiveness of internal processes put into place in each of the participating companies that ensure that they advance human rights, freedom of expression and user privacy in the course of doing business. Other markers of success include the contribution of participants to multi-stakeholder collaboration and learning, engagement in public policy, collective responses to emerging issues, and the building of global partnerships. A collaborative effort is underway to develop evaluation methods and tools for companies to carry out human rights assessments before introducing new products and services or entering new markets. The accountability processes put into place at the GNI are designed to create a strong basis for monitoring progress and to provide strong incentives for companies to follow through on their commitments, both individually and collectively. The expectation is that GNI members will share information and best practices that will assist companies in evaluating these difficult questions where clear answers are elusive.

The objectives and processes that guide the operation of the initiative are codified in a series of documents released at the launch. The Principles document lays out the commitments of the members to collaboratively promote freedom of expression and privacy online. These Principles also provide high-level guidance for the member organizations. Implementation Guidelines provide detailed guidance to ICT companies for putting the Principles into practice and provides the institutional framework for collaboration among companies, NGOs, investors and academics. The Governance, Accountability and Learning Framework sets out a multi-stakeholder governance structure, goals for collaboration and a system of company accountability to support the Principles, maximize opportunities for learning and ensure the integrity and efficacy of the Initiative. The group is in the process of finalizing a Governance Charter that will define the membership of the board and provide detailed direction on the procedures for implementing the accountability measures.

The GNI constitutes a unique forum for information sharing, learning and deliberation. Perhaps the most impressive accomplishment to date is the deep trust that has emerged among the participants acting towards a common cause. The record of collaboration, collective advocacy, and sharing of knowledge and ideas are remarkable in light of the diverse backgrounds and fierce competition that has characterized the prior relationship of the participants. The exchange of information among participants has improved the understanding of the complex processes at work for each of the individual organizations and the GNI. In addition to putting the organizational structure of the initiative in place, since launch, GNI members have been actively engaged in collaborating around emerging issues, including Green Dam and intermediary liability, among other issues. Further details can be found at: http://www.globalnetworkinitiative.org/issues/index.php This initiative is expected to be an important forum for identifying emerging issues with the hope that conflicts in law and expectations can be avoided.

Much work lies ahead for the GNI. Although the current members of the GNI are respective leaders in their field, they still constitute a small proportion of the companies and organizations around the world that collectively shape global Internet freedom. Planning is underway for outreach and public events designed to expand membership of

the initiative to include additional technology companies and human rights groups, with a focus on global reach and diversity.

While we place high hopes on the capacity of the GNI to play a leadership role in helping to resolve these international tensions over human rights online, it is too soon to evaluate the ultimate effectiveness of the organization.

Recommendations for Moving Forward

The future of online freedom of expression and privacy in China will be shaped within China; the Chinese themselves will determine the pace, direction and future of online freedom of expression and privacy in China. If there is to be progress on these issues, it will take many years to enact. While we must recognize the limited influence of U.S. companies, non-profits and government, we must also acknowledge that their role is important. Long-term engagement is likely to be the most productive intervention. As we have seen in the recent policy shift with Green Dam, Chinese authorities are not immune to popular opinion within China and global criticism.

The US government can and should play a constructive role in helping companies to navigate this difficult landscape. In this spirit, I offer some preliminary suggestions for your consideration:

Expand multilateral dialogue and inter-governmental cooperation
Facilitating a formalized process for delivering law enforcement requests that involves inter-governmental cooperation would help companies to extricate themselves from the impossible task of evaluating the legitimacy of law enforcement requests.

Provide support for the GNI
The promising steps taken by the GNI should be supported. The government should offer encouragement and incentives for greater participation in the GNI and provide venues for dialogue between the government and GNI members, including not only current members but also prospective members.

Encourage greater transparency and information sharing
Crafting effective responses to international threats to freedom of speech and privacy online is contingent upon understanding the nature, scope and nuances of these threats. Technology companies, academic and research institutions, shareholders and investment enterprises and advocacy organizations each contribute important perspectives and sources of information. The US government can play a vital role in investing in research in support of these efforts, and providing incentives for transparency and information sharing among companies committed to these issues.

Lead by example
Balancing the exigencies of law enforcement with freedom of expression and privacy online presents difficult challenges for any country. The United States should be an example for China and the rest of the world.

After extensive study of this issue, I have concluded that the best levers of influence at this point are persuasion, diplomacy, dialogue, and transparency in supported by collective deliberation and action, not legislation.

Filename: Faris_USCC testimony
Directory: C:\Documents and Settings\Jertman\Local Settings\Temporary Internet Files\OLK5E
Template: C:\Documents and Settings\Jertman\Application Data\Microsoft\Templates\Normal.dot
Title: Intro –
Subject:
Author: rfaris
Keywords:
Comments:
Creation Date: 10/1/2009 7:48:00 PM
Change Number: 8
Last Saved On: 10/2/2009 7:05:00 AM
Last Saved By: rfaris
Total Editing Time: 60 Minutes
Last Printed On: 10/6/2009 12:35:00 PM
As of Last Complete Printing
Number of Pages: 9
Number of Words: 3,715 (approx.)
Number of Characters: 21,140 (approx.)