



COMMITTEE ON INTERNATIONAL RELATIONS  
UNITED STATES HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON AFRICA, GLOBAL HUMAN RIGHTS AND  
INTERNATIONAL OPERATIONS

and

SUBCOMMITTEE ON ASIA AND THE PACIFIC

February 15, 2006

Written Statement of:

John G. Palfrey, Jr.

Clinical Professor of Law & Executive Director  
Berkman Center for Internet & Society, Harvard Law School

Mister Chairman, Distinguished Members of the Committee:

I applaud the Committee's leadership in drawing attention to the relationship between the Internet and human rights in China and the several dozen other states around the world that censor and practice surveillance of Internet-based communications. I submit this written testimony today as a member of a team of researchers, called the OpenNet Initiative, that has been conducting empirical testing of China's Internet filtering regime for the past several years and monitoring the involvement of United States companies in that regime. My colleagues Ronald Deibert of the University of Toronto, Rafal Rohozinski of the Advanced Network Research Group of the Cambridge Security Program, University of Cambridge, and Jonathan Zittrain of the University of Oxford and Harvard Law School, are also principal authors of the OpenNet Initiative's work. We have also studied in depth the filtering regimes of states in the Middle East, the former Soviet republics, and parts of East Asia. We have studied the case of China in particular, as it is much the most extensive online censorship regime in the world.

The United States Congress, human rights activists, academics, and United States technology companies all ought to share a common goal: to promote the growth of the global, public, unitary, network of networks that is the Internet and to foster the many positive effects that this network brings with it. The spread of Internet technologies that operate on the "end-to-end principle" – or on the basis of "network neutrality," which means that Internet traffic is not stopped between point A and point B – have proven their mettle to serve not only our economies, but also our cultures and our democracies, if well-maintained and put to their highest and best use. The way to achieve these common goals is neither for the United States technology industry to turn its back on doing business in markets such as China, nor for the Congress to ban such activity outright.

The hard question is how to fashion a policy environment in which the engagement is done in an ethical manner, a manner that upholds the values that we hold dear as

Americans. The right to free expression and the right to privacy – in particular, the honoring of these rights when political activity is at stake, often the political activity of dissidents – are values that lie at the core of our republic. Our respect for these values is essential, too, to our interaction with the rest of the world – including China and many other regimes where these values are honored to lesser extent or in different ways.

The problem that United States technology companies face in doing business in China, and in doing business in the three dozen or more countries that extensively practice filtering and online surveillance, is well-established. While China seeks to grow its economy through the use of new information and communications technologies, the Chinese state has demonstrated its fear of disruptive effects of free and open communications made possible by the Internet – particularly on topics that relate to human rights and to political activism. This fear has led the Chinese government to create the world's most sophisticated Internet filtering and surveillance regime. One of the topics commonly blocked is information related to human rights, including the website of the respected NGO, Human Rights Watch.

The job of the Internet censor is a very hard one. Determined technologists, in China and elsewhere, can get around every Internet filtering and surveillance regime established to date. Some Chinese have described the effect of the Internet filtering regime as a high-tech screen door: the state seeks to let in the sunlight, but keep out the bugs. No matter what, the system will be imperfect.

It is the imperfection of these regimes that give rise to both the problem and the opportunity facing United States technology companies.

The problem is that the Chinese state needs as many players in the value chain – as many people who operate points of control on the network – to assist in the censorship and surveillance regime as possible. The Internet is a distributed network; as a factual matter, control of the network, too, is best carried out on a distributed basis. The Chinese state expects United States technology companies – as well as Chinese technology companies – that operate in China to participate in the distributed process of controlling the information environment. The trend in this direction is nearly certain to continue, absent other factors that radically change the situation.

The opportunity that lies before United States technology companies is that their directors and officers and employees do care about the right to free speech and privacy. In an imperfect censorship and surveillance regime, there are gray areas. The Chinese legal regime is not all that precise when it comes to what is expected of any of the intermediaries in the value-chain of the Internet. It is in these gray areas that United States technology companies might be able to make a difference from the perspective of democracy. Working together, working with United States policy-makers, and like-minded companies and policy-makers from other places around the world, there is a great deal that can be done in these gray areas.

One specific example: as the OpenNet Initiative has shown through its research, domestic Chinese blog software providers filter content that is posted to weblogs hosted in China (<http://www.opennetinitiative.net/bulletins/008/>). The law in China does not state the precise kind of filtering that these weblog providers must employ. If United States companies that offer blog software in fact establish less restrictive means of enabling Chinese bloggers to write about sensitive topics in their blog posts, then their

argument that their technologies result in a more open information environment would resonate.

There are ethical lines to be drawn in the gray areas of filtering and surveillance regimes – lines that will distinguish, or better yet bring together in common cause, technology companies that are doing business in China. The drawing of these lines, ideally in a collaborative fashion, will help to shape sound public policy on this matter.

### **A Code of Conduct**

Private technology companies cannot today participate in these marketplaces without consequences based upon their actions. Human rights are implicated. Companies in this position have an obligation to figure out what it means to act ethically when they are doing business in a place like China. They also have a self-interest in having a common code of practice to which they can point and rely upon in resisting abusive filtering and surveillance requests. The United States Congress is right to pay attention and to provide the kind of leadership that will result in action – pro-democratic action – on the world stage.

The most promising next step is for industry leaders to work together, perhaps in concert with the human rights and academic communities, to adopt a voluntary solution to the problem – to establish a common ethical pathway.

A group of academics studying this issue – at the Berkman Center at Harvard Law School, the University of California-Berkeley, University of Toronto, the Oxford Internet Institute at the University of Oxford, University of Cambridge, and the University of St. Gallen in Switzerland, among others – have begun working together to develop of a set of principles that would guide businesses that are offering services in states that filter extensively and spy on Internet conversations and give them a base of support for resisting abusive surveillance and filtering requests.

There are a number of things that United States technology companies can do to make their actions more transparent to users, more protective of civil liberties, and more accountable to all of us. Microsoft, Yahoo!, Google, and Cisco each should be applauded for their respective, increasingly clear public statements about how they will operate moving forward when it comes to doing business in China. These public statements, and action based upon these statements, are essential to moving forward toward a solution.

### **Legislation and Other State Action**

Second, it may be the case that the Congress, or other branches of the United States government, must take new action to solve this problem. That said, any outcome that bans United States technology companies from doing business in China, in the long-run, would not be in the best interests of democracy there or in states with similar Internet policies.

There are many other options beyond an outright ban that could help, if it is clear that the industry cannot solve its own problem. This issue of censorship and surveillance should be the Administration's top priority with respect to global Internet governance discussions, which have to date focused on the policy backwaters of the functioning of

the domain name system. This issue – ultimately, a key issue of human rights and of the development of well-functioning democracies around the world – should be a top priority in trade negotiations, not an after-thought.

As a last resort, the Congress could develop a corollary to the Foreign Corrupt Practices Act that would guide – and tie the hands of – United States technology companies doing business under these circumstances. Such a step is risky on many levels, raises thorny questions of sovereignty, and should be taken only with great care.

We ought to see this issue not as a crisis, but rather as an opportunity. Internet technologies, developed by the likes of Microsoft, Yahoo!, Google, Cisco, and many others, are doing terrific things for democracy around the world. At the same time, the People's Republic of China's Internet filtering and surveillance regime has the greatest effect on the freedom of expression, and on the efforts of human rights workers, of any filtering regime throughout the world. The best outcome would be for our technology companies to be able to compete in these marketplaces – with their best-in-the-world offerings – without having to compromise our values and without having to become complicit in Internet censorship and surveillance.

We need to come together to figure out how to ensure that these companies and their technologies are indeed a force for greater democratic participation, not pushing against it. These companies should be, and can be, the darlings of the human rights community for what they can do for human rights in places like China. It doesn't happen to be the case today, but I have no doubt that we can get to that point through collaboration that is grounded in honesty, openness, transparency, and a commitment to bedrock democratic values.

*-- end of written testimony --*

## Appendix:

### Topics Censored by the Chinese Filtering Regime.

Members of the OpenNet Initiative have been studying China's Internet filtering and surveillance regime since 2002. Our studies have shown that China's online censorship systems are by far the most sophisticated and extensive in the world.

China filters Internet content on a broad array of topics. The censors particularly target sensitive political topics for blocking. To determine precisely what is blocked, we created a keyword list of terms on sensitive topics, such as the Falun Gong spiritual movement, the Taiwanese independence movement, and criticism of China's government and leaders. We used the Google search engine to compile a list of large numbers of sites related to these keywords. Our volunteers then attempted to access these sites from within China using our testing application.

Some of the most noteworthy of the topics censored include, as of our 2005 testing:

- Information online related to opposition political parties (more than 60% of Chinese-language sites tested were blocked);
- Political content (90% of Chinese-language sites tested on *The Nine Commentaries*, a critique of the Chinese Communist Party, and 82% of sites tested with a derogatory version of Jiang Zemin's name were blocked);
- The Falun Gong spiritual movement (44 – 73% of sites tested, in both English and Chinese languages);
- The Tiananmen Square protest of June 4, 1989 (at least 48% of Chinese-language sites tested, and 90% of sites related to the search term "Tiananmen massacre");
- Independence movements in Tibet (31% of tested Chinese-language sites), Taiwan (25% of tested Chinese-language sites), and Xinjiang province (54% of tested Chinese-language sites); and,
- Virtually all content on the BBC's web properties and much of the content published online by CNN.

Our testing also found evidence that China tolerates considerable overblocking – filtering of content unrelated to sensitive topics, but located at URLs or with keywords similar to these subjects – as an acceptable cost of achieving its goal of controlling Internet access and publication. China has managed over time to reduce the rate of overblocking as its filtering technologies have improved.

### Types of Communications Affected by China's Filtering Regime.

China's commitment to content control is revealed by the state's efforts to implement filtering for new methods of communication as they become popular. Most states that

filter the Internet do an ineffective job of blocking access to certain web sites, and stop there.

While China's blocking of World Wide Web sites is well-known, much less is known about the extent to which China blocks other forms of Internet-based communications. As Web logs ("blogs") became popular in 2004, the state initially closed major Chinese blog service providers until they could implement a filtering system. When these providers re-opened, their service included code to detect and either block or edit posts with sensitive keywords. Similarly, on-line discussion forums in China include both automated filters and human Webmaster inspections to find and remove prohibited content. Most recently, China moved to limit participation in university bulletin board systems (BBS) that had featured relatively free discussion and debate on sensitive topics. The Chinese filtering regime also causes the blockage, or dropping, of e-mails that include sensitive terms. Our testing of e-mail censorship suggests that China's efforts in this area are less comprehensive than for other communications methods, though reports from the field suggest that the fear of surveillance and blockage of e-mails is a serious issue for many activists regardless of the precise extent of the censorship itself.

One of the most intriguing questions, as yet unanswered, is whether emerging new technologies will make Internet filtering harder or easier over time. A new, emerging crop of more dynamic technologies – centered on the fast-growing XML variant RSS, which is a means of syndication and aggregation of online content, such as weblog entries and news stories from major media outlets – should make filtering yet harder for the Chinese and for other countries that seek to control the global flow of information. The cat-and-mouse game is certain to continue.

#### The Legal Context of Filtering in China.

China's intricate technical filtering regime is buttressed by an equally complex series of laws and regulations that control the access to and publication of material online. While no single statute specifically describes the manner in which the state will carry out its filtering regime, a broad range of laws – including media regulation, protections of "state secrets," controls on Internet service providers and Internet content providers, laws specific to cybercafés, and so forth – provide a patchwork series of rationales and, in sum, massive legal support for filtering by the state. The rights afforded to citizens as protection against filtering and surveillance, such as a limited privacy right in the Chinese Constitution, which in other situations might provide a counter-balance against state action on filtering and surveillance, are not clearly stated and are likely considered by the state to be inapplicable in this context. For the most part, the Chinese legal regime is not transparent, in the sense that it does not describe the filtering regime. The pronouncement by a Chinese state spokesman on February 14, 2006, on the day before these hearings, that discussed the filtering regime in its international context, was a rare public acknowledgement of the filtering regime's existence.

Our analysis of China's legal regime indicates a significant expansion in the number of statutes, regulations, and regulatory bodies involved in oversight and control of Internet access and content since 2000. These rules often appear to be arbitrary and are certainly extraordinarily burdensome, such as rules that call for multiple licensing and registration requirements imposed upon Internet content providers.

China's legal system imposes liability for prohibited content on multiple parties: the author who creates it, the service provider who hosts it, and the end user who accesses it. This combination of transaction costs and broad liability has a substantial chilling effect on on-line communication.

We are cognizant that, while we have taken great care in our legal analysis of China's filtering regime as it appears on the books, our report may not describe the law as it applies on the ground. Political stability is clearly more important than legal justification for the state's actions, as a comparison of China's filtering regime to the corresponding legal framework demonstrates.

#### A Comparison of China with Other States that Filter.

Our studies have compared the Internet filtering practices of a series of national governments in a systematic, methodologically rigorous fashion. A primary goal of this research is to reach useful, substantive conclusions about the nature and extent of Internet filtering in states that censor the Internet and to compare practices across regions of the world. Over the course of the next several months, we will release a series of extensive reports that document and provide context for Internet filtering, previously reported anecdotally, in each of the dozen or so countries that we have studied closely. The new reports released to date – which document filtering in Saudi Arabia, the United Arab Emirates, and Bahrain as well as in China – will be followed shortly by other studies of other states in the Middle East, East Asia, and Central Asia.

Filtering regimes – and their scope and level of effectiveness, respectively – vary widely among the countries we have studied. Filtering is practiced at some level by most countries; it is best thought of as a continuum of behavior rather than a binary, on-off approach to content control. Some countries employ only symbolic filtering, and depend on legal or social pressures to constrain content. These states include Bahrain and Singapore, which block only a few sites that are primarily pornographic in nature. Other countries demonstrate limited blocking but, because of an unsophisticated approach to filtering, also censor large numbers of unrelated sites. This inadvertent filtering, known as “overblocking,” was demonstrated by South Korea when it sought to prevent access to sites promoting North Korea. Finally, many countries employ a mix of commercial software (from American companies such as Secure Computing and Websense) to control content such as pornography and gambling while also customizing their block lists to target prohibited political, religious, and social content.

China, as documented in a number of studies and supported by the our findings, institutes by far the most intricate filtering regime in the world, with blocking occurring at multiple levels of the network and covering content that spans a wide range of topic areas.

A complete study of Internet filtering in China, as of 2005, may be found at <http://www.opennetinitiative.net/china/>.

*The OpenNet Initiative is a collaborative partnership between three leading academic institutions: the Citizen Lab at the Munk Centre for International Studies, University of Toronto; Berkman Center for Internet & Society at Harvard Law School; and the Advanced Network Research Group at the Cambridge Security Programme, University of Cambridge.*