April 14, 2005

Written Statement of:

John G. Palfrey, Jr.
Executive Director, Berkman Center for Internet & Society, Harvard Law School

Before the U.S. – China Economic and Security Review Commission
Hearing on China's State Control Mechanisms and Methods

Mister Chairman, Madame Co-Chair, Distinguished Members of the Commission:

My name is John Palfrey, and I am the executive director of the Berkman Center for Internet & Society at Harvard Law School, where I also teach on Internet-related subjects as a Lecturer on Law. I am a member of a team of researchers, called the OpenNet Initiative, based at the University of Toronto, the University of Cambridge, and Harvard Law School, that has been conducting rigorous empirical testing of China's Internet filtering regime for the past several years. The report we present to you today builds on a similar report we released in 2002. My colleagues Ronald Deibert of the University of Toronto, Rafal Rohozinski of the University of Cambridge, and Jonathan Zittrain of Harvard Law School are also principal authors of this report. We have also studied in depth the filtering regimes of states in the Middle East, the former Soviet republics, and parts of East Asia. I am joined today by my colleagues Nart Villeneuve, the Director of Technical Research at the Citizen Lab at the University of Toronto, and Derek Bambauer, a research fellow at the Berkman Center at Harvard Law School.

Today the Commission considers China's mechanisms and methods of state control. While China seeks to grow its economy through use of new technologies, the state's actions suggest a deep-seated fear of the effect of free and open communications made possible by the Internet. This fear has led the Chinese government to create the world's most sophisticated Internet filtering regime.

The People's Republic of China has the most extensive and effective legal and technological systems for Internet censorship and surveillance in the world today. China's system prevents users from accessing most politically sensitive content on the Internet, including information about opposition political groups, independence movements, the Falun Gong spiritual movement, the Dalai Lama, and the Tiananmen Square incident. China's system blocks virtually all BBC content and much CNN content online. The Chinese government has imposed significant legal and technical restrictions that prevent the publication of and access to content sensitive to the government.

China's filtering has advanced far beyond the comparatively limited filtering regimes in place in other states and, since we last tested China's filtering systems in 2002, its approach has become markedly more sophisticated and successful. The success of China's filtering efforts lies in its reliance on multiple, overlapping filtering methods and systems. China's filtering takes place at multiple levels, including at access points such as cybercafés, at intermediaries such as Internet Service Providers (ISPs), and at the national Internet backbone network.

China employs a mixture of soft and hard controls to limit the Internet material its citizens can access. Hard controls include technical measures such as keyword and source blocking. Soft controls include both extra-legal measures, such as informal pressure on users and content providers, and formal legal measures, such as broad and often arbitrary-seeming legal restrictions combined with zealous enforcement. China's legal enforcement measures concentrate primarily on the creation and dissemination of content rather than its retrieval. Thus, these soft controls create a "chilling effect" that deters users, and intermediaries such as ISPs, from posting content on sensitive or prohibited topics.

Since we last tested, China has broadened its controls over the Internet through expansion of both laws and technology. Legally, new requirements and restrictions raise barriers to creating and hosting sensitive content, placing authors and intermediaries on notice that their actions are monitored. Technologically, China's filters have become more sophisticated, with improved targeting of prohibited content and less "overblocking" of similar but less sensitive materials. As new Internet communications methods have become popular in China – for instance, on-line discussion forums, search engines, and Web logs – the Chinese state has extended its filtering apparatus to control expression in these media. Filtering systems have also become integrated into the architecture of new technologies. Chinese blog providers, for example, include code to prohibit publication of sensitive terms and content.

The Chinese state's filtering systems lack transparency in nearly every sense. In addition to limiting what Chinese citizens can come to know about the censorship process, this lack of transparency complicates the task of monitoring its filtering regime. Most important, this lack of transparency contributes mightily to the climate of self-censorship. Chinese officials very rarely admit that the state censors Internet content. Officials do not disclose at any level of granularity what material it targets through the filtering regime. Unlike Saudi Arabia, for instance, China does not permit users to participate in blocking decisions or to appeal erroneous filtering of sites that do not include content intended to be blocked.

China's Internet filtering and censorship efforts have global ramifications, and should be of concern to Internet users worldwide. Most of all, the ramifications of this censorship regime should be of concern to anyone who believes in participatory democracy – online and offline. China's growing Internet population represents nearly half of all Internet users worldwide, and will soon overtake the United States as the single largest national group of Internet users. How the Chinese government restricts its citizens' online interactions is significantly altering the global Internet landscape. China's advanced filtering regime presents a model for other countries with similar interests in censorship to follow. China acts as a regional Internet access provider for states such as Vietnam, North Korea, Uzbekistan, and Kyrgyzstan. Through this important role as a gatekeeper between citizens in other states and the Internet, China may be able to share or export its content controls to neighboring states and their local Internet service providers. There is no reason to believe that the Chinese government will refrain from exporting its filtering technology to other states, if the opportunity arises.

While it may be an open question as to whether democratization and liberalization are taking place in China's economy and government, there is no doubt that neither is taking place in China's Internet environment today.

The OpenNet Initiative's Methodology for Studying Internet Filtering in China.

Members of our consortium have been collecting data on China's Internet filtering regime since 2002. The data included in this report have been updated as recently as this week. As the Chinese government has developed more sophisticated means of filtering, we too have developed more sophisticated and comprehensive means of testing their filtering efforts. Since our last study, our testing methods have become substantially more fine-grained and reliable.

To gauge how Internet filtering likely affects the average Chinese Internet user, ONI employs a variety of means to test blocking and censorship and to ensure data integrity. We test filtering from different points on China's network, in different geographic regions, across time. The resulting data allow us to conduct rigorous longitudinal analysis of Internet blocking in China. We examine both the response that users receive from the network and from the Web servers involved and information about the route that a request takes on its way from a user to a Web server – allowing us to pinpoint exactly where information is censored and controlled. While it is impossible to paint a flawless picture of China's Internet filtering efforts at any given time, we are increasingly confident that our data present an accurate snapshot of China's Internet filtering regime today.

We have tested China's Internet filtering regime using four methods. Under Nart Villeneuve's leadership, ONI developed and deployed an application to test within China what content is, and is not, blocked by the state's system. Volunteers installed and ran this application on their home computers to allow ONI to probe China's filtering from a wide range of access points inside the country. Our volunteers also ran manual checks for access to web sites.

Second, we accessed proxy servers in China to duplicate and augment this in-state testing of whether or not a citizen could access a certain web site. Proxy servers are points in China's network that act to aggregate and respond to user requests for content. Accessing a proxy server in China allows ONI to browse the Internet as though we were in China, even though we are physically located in another country. Through proxies, we are able to obtain a random sampling of Web content – and censorship – across multiple networks and service providers.

We have also explored whether China blocks other types of Internet-related communications. Anecdotal evidence has suggested for a long time that China blocks certain e-mail communications and that Web logs – or "blogs", which are personal online journals, often kept by increasingly famous activists – have been more recently targeted by the Chinese government for blocking.

To test these hypotheses, we published content on blogs on three of China's most popular blog providers to evaluate the services' keyword filtering mechanisms. We then later sought to access this blog content that we had published.

Finally, we sent a series of test e-mail messages to, and from, accounts hosted by several Chinese ISPs. These messages contained content on sensitive topics – such as political dissidents, objections to the state's repression of the Tiananmen Square protests, and religious persecution – typical of e-mails sent by human rights organizations.

In addition to employing these technical methodologies, we have closely studied the legal and policy regimes in place in China. The insights of many scholars and activists, both inside China and elsewhere, guided our research and provided quality assurance.

Topics Censored by the Chinese Filtering Regime.

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:

- 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.

China has issued official statements about its efforts to limit access to Internet pornography. However, we found that less than 10% of sites related to searches for the keywords "sex," "pornography," and "nude" were blocked. This imprecision, when compared either to the effectiveness of China's censoring of political content or to the relatively thorough blocking of pornographic materials by states in the Middle East, suggest that blocking pornography is nowhere near the imperative that controlling political speech is in China. It also suggests that China's war on pornography may be focused more on closing domestic sources of pornography than on filtering foreign sites that are providing pornographic content.

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 will 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.

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. Though its filtering program is widely discussed, Singapore, by contrast, blocks access to only a small handful of sites, mostly pornographic in nature. Most other states that we are studying implement filtering regimes that fall between the poles of China and Singapore, each with significant variation from one to the next. These filtering regimes can be properly understood only in the political, legal, religious and social context in which they arise.

Conclusion.

By any means of comparison, the People’s Republic of China’s Internet filtering regime has the greatest effect on the freedom of expression of any filtering regime throughout the world.

The Chinese censors have a very difficult job as they try to contain the flow of information on the Internet. The most determined Chinese Internet users can often elude the censors in nearly all instances. But the Chinese censors are head and shoulders above everyone else – short of those who block access to the network altogether – in terms of filtering the Internet. Most citizens see a very different Internet in China than citizens in other places around the world.

The Chinese Internet filtering regime grows more robust each day. As new information and communications technologies develop, the Chinese censors track the technologies and determine means to control the freedom of expression through the new media. Filtering and efforts to circumvent it are likely to continue into the foreseeable future. Though far from completely effective, China’s filtering regime achieves a climate of self-censorship and a chilling of expression and communications online, particularly when it comes to political dissent.

The Internet can be an extraordinarily empowering tool. Individuals who have never before had a voice – whether in China or anywhere else that the network reaches – can today project their voice to a world-wide audience. Seen from another vantage point, the way citizens use the Internet is a threat to the political stability of the governing Communist Party in China. The state’s Internet filtering regime is intended to mitigate this threat.

If deployed properly, the Internet can help foster active, participatory democracies throughout the world. Internet filtering and surveillance, most clearly exemplified by China’s Internet filtering regime, threaten to choke this potential.

* * *

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