Written Statement of:

Ronald J. Deibert
Associate Professor of Political Science, Director, the Citizen Lab
Munk Centre for International Studies, University of Toronto
June 18, 2008

Distinguished members of the Commission:

I would like to offer my sincere appreciation for the invitation to appear before the U.S.-China Economic & Security Review Commission. In a world of increasingly urgent global problems, from poverty and environmental degradation to weapons of mass destruction, it is essential that governments recognize and promote an unfettered medium of communication through which citizens around the world can access information of their own choosing, speak freely, and debate and share ideas. The Internet is the closest we have today to such a medium, but its openness and accessibility are very much under threat. Even as the number of Internet users expands worldwide, access to information and freedom of speech are being strangled and degraded by censorship, surveillance, and militarization. Congressional investigation at any level concerning these issues is a very welcome development.

My name is Ron Deibert. I am an associate professor of political science and the director of the Citizen Lab at the Munk Centre for International Studies, University of Toronto. The Citizen Lab focuses on advanced research and development at the intersection of the Internet, global security, and human rights. I am one of the founders and principal investigators of the OpenNet Initiative, a collaborative project among the Citizen Lab and the Universities of Harvard, Cambridge, Oxford, as well as numerous non-governmental organizations and individual partners worldwide. The aim of the ONI is to document patterns of Internet censorship and surveillance across the globe. Since 2003, when the ONI started, we have produced eleven major country reports, including two on China; produced the world's first truly global comparative study of Internet content filtering, recently published in the volume *Access Denied*[1]; and we are presently testing in over 70 countries. For the last several months, our researchers within and outside China have been carefully investigating Internet content filtering, and we intend to issue a detailed report later this year.

In addition to being one of the core partners of the ONI, the Citizen Lab has also developed one of the world's leading software tools to help people get around Internet censorship, called "psiphon." A freely available and open source tool,

---

[1] Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT Press, 2008).

psiphon has been used extensively to help citizens evade content filters and exercise their human rights of access to information and freedom of speech. We are presently working on an enterprise-level version of psiphon that will cater to the requirements of large organizations, such as global media, thus facilitating access to information for journalists who will be covering the Olympic games in Beijing later this year.

Lastly, I am one of the principal investigators of the Information Warfare Monitor Project (IWMP), a collaboration among the Citizen Lab, Cambridge University, and the SecDev Group whose aim is to monitor the emergence of the Internet as a domain for military and intelligence operations in support of political objectives. Led by my colleague Rafal Rohozinski of Cambridge University and the SecDev Group, the IWMP has initiated several workshops and studies involving US, UK, Russian, and Chinese military and intelligence personnel on this newly emerging yet vital terrain of state competition. In my capacities as principal investigator of the ONI and the IWMP, and director of the psiphon project, I can offer a unique perspective on China's Internet censorship regime and the ways in which it can be evaded and resisted.

China's Internet Content Filtering Regime

Like most countries that engage in Internet content filtering that the ONI has studied, China's censorship practices lack transparency and public accountability. Official acknowledgement of these practices has been inconsistent at best, deceitful at worst. Most times officials deny or do not discuss details of content filtering practices. On rare occasions when public officials raise the subject, it is justified in terms of protecting public safety, core social values and stability, and compared to similar filtering practices in the West. However, the full scope of China's censorship regime is never spelled out in official circles or public government documents.

What we do know of China's Internet filtering regime comes from the activities of bloggers, academics, and non-governmental organizations, like Human Rights Watch, Amnesty International, Reporters Without Borders, Human Rights in China, and many others both within the PRC and outside. The ONI is very much embedded in this thriving civil society community which constantly monitors China's filtering system and compares and discusses its characteristics on email lists, blogs, and other public forums.

The ONI is distinguished from these other organizations by the robust and careful methodology that we employ in documenting patterns of Internet censorship. The ONI's methodology blends "technical Intelligence" that yields quantitative data with field based contextual research that helps target technical tests and interpret results. The technical data is derived from a suite of software tools that are deployed by researchers in countries under investigation which

connect back to databases maintained by the ONI and check accessibility to thousands of websites, keywords, and services in local and English languages. Forensic investigations of the results, combined with tracing and mapping of network connections, determine what is being blocked, where the block is implemented, and often the technology that is being used to do the blocking. Country experts then analyze the results and place them in their wider social and political context to give a comprehensive picture of a country's filtering policies and practices.

The ONI has released two major reports on China's filtering regime so far, both of which are free and accessible on our website (http://opennet.net/). A third report is presently underway and will be released later this year. Our extensive 2005 report described China as operating "the most extensive, technologically sophisticated, and broad-reaching system of Internet filtering in the world"[2] and I believe that conclusion remains the same today. China's filtering regime employs a combination of technical, legal, and social measures that are applied at a variety of access points and overseen by thousands of private and public personnel and which together filter content sent through a range of communication methods, such as websites, blogs, forums, and email. Together, these measures create a matrix of soft and hard controls and induce a widespread climate of self-censorship.

Technical filtering mechanisms can be found at all levels of the Internet in China, from the backbone to PCs located in hotels and Internet cafés. Although ISPs, Internet cafés, search engines and other network services, can and do operate their own filtering systems, all network traffic is subject to a uniform system of filtering at three major international gateways (located in Bejing, Shanghai, and Guangzhou). Our research has uncovered three forms of filtering at these international gateways: DNS tampering, keyword filtering, and IP blocking.[3] DNS tampering works by interfering with the system that cross-references domain names with the numerical address associated with them. Users are directed to an invalid IP as if the site they requested did not exist. By contrast, IP blocking targets the numerical address. This type of blocking can cause major collateral filtering of unrelated content because different domain names can share the same IP address host. Keyword filtering targets the URL path (and, we suspect, increasingly the body of the web page as well) searching for banned terms. Upon finding one, the routers send what are known as "RST packets" that terminate the connection between sending and receiving computers, effectively penalizing that computer from making requests to the same server for an indefinite period of time. Since the system works both ways

[2] The ONI, *Internet Filtering in China 2004-2005, A Case Study*, (April 2005). Retrieved May 22, 2008 from http://opennet.net/studies/china

[3] See Stephanie Wang and Robert Faris, "Welcome to the Machine," *Index On Censorship*, (Volume 37, Issue 2 May 2008) , pages 106 – 113 for a detailed overview.

(for requests exiting and entering China) it can be tested by searching for banned keywords, like "falun" on search engines hosted in China (e.g., Baidu.com). In each case listed above, users making requests for banned information receive an error message on their web browser, making it appear as if the information is not available or there is something wrong with their Internet connection. In other words, users in China trying to access banned content do not receive a block page informing them that the content is officially filtered, as is the case in some other countries that censor the Internet. Our tests have shown filtering is centralized and largely consistent across each of the international gateways; no matter the ISP or café from which you connect in China, this gateway level of filtering is an unavoidable last line of defense.

The type of content that is targeted for blocking is wide-ranging and covers social, cultural, security, and political topics considered a threat to communist party control, and social and political stability. As our report summarized, "Chinese citizens seeking access to Web sites containing content related to Taiwanese and Tibetan independence, Falun Gong, the Dalai Lama, the Tiananmen Square incident, opposition political parties, or a variety of anti-Communist movements will frequently find themselves blocked."[4] Websites and services that help people evade government censorship are also regularly filtered. Our tests also show that China's filtering tends to focus disproportionately on content in local Chinese languages. Users searching for the equivalent English language terms, for example, will often get a higher proportion of results than the same terms searched for in Chinese.

Although the filtering system appears consistent and relatively stable across time, the Chinese government has also demonstrated a propensity to use what we have called "just-in-time" blocking in response to special situations as they emerge. For example, during demonstrations in Tibet, China implemented new blocks against Youtube.com and other video-streaming services that were circulating images of protests, and then lifted them subsequently. The Tibetan protests also point to another, newly sophisticated form of blocking emanating from China: the use of distributed denial of service (DDOS) attacks. There have been persistent and increasing charges that DDOS attacks against servers in the United States, United Kingdom, Canada, and elsewhere have their origins in Mainland China. Such attacks have been especially prominent during and following the demonstrations in Tibet, with the servers of many Tibetan and Chinese human rights organizations systematically targeted. These more "offensive" methods of denying access to information by effectively targeting and disabling the sources of information themselves (rather than passively blocking requests for information, as the filtering systems do) are especially concerning because it is difficult to pinpoint the source of the attacks. Distinguishing the involvement of government officials from vigilantes is very

---

[4] Ibid.

difficult, as the methods involved are dispersed, opaque and allow for a degree of plausible deniability. They also present challenges for monitoring organizations like the ONI whose methods are calibrated to document passive filtering techniques and not information attacks of the type described above.

Technical means of filtering are complemented by an extensive set of social and legal or regulatory measures. Legal or regulatory measures tend to be vague and generally written, thus offering wide scope for application and enforcement, and uncertainty among users. Most have the affect of devolving responsibilities to end users and services, like café operators, ISPs, blog hosting services, and media, to be responsible for policing the content they post and that which they host. Since enforcement can be arbitrary, users and operators of services tend to err on the side of caution preferring to prevent or remove offending material rather than risk censure. Social measures are even more general, and thus harder to define, but include operating norms, principles, and rules which are propagated through media and official channels, and are combined with extensive techniques of surveillance, which together affect behavior in both formal and informal ways. These include self-discipline pacts signed by Chinese Internet service companies pledging to uphold public values, and the cartoon police officer characters "Jingjing" and "Chacha" that popup and warn users not to visit banned sites or post harmful information.

The Beijing Olympics

There is considerable speculation as to how the Chinese government will deal with Internet controls during the upcoming Olympic games in Beijing. At least 30,000 foreign journalists are accredited to the Olympic games, and Beijing is contractually obliged to the International Olympic Committee to provide free Internet access for them. How and whether that will be accomplished is so far unknown, but there are several possible scenarios short of the unlikely rolling back of all filters. For example, China may reduce or eliminate controls over access to popular English language websites, news services, and blogging platforms, while keeping in place or even enhancing filters on the local language equivalents. This policy would give outsiders the impression that restrictions are minimal while targeting those sources of information that matter most for domestic policy. Already there is evidence that such a policy has begun, with long-standing restrictions on the English language version of the BBC news now lifted while the Chinese version of BBC remains inaccessible to users in China. China may also set aside a block of IP addresses for journalists that the routers will ignore; it is unclear, however, how that system would work for journalists accessing the Internet through multiple locations while traveling, such as in Internet cafés outside of official Olympic sites. Whatever method is ultimately employed, it seems highly probable that after the Olympics the controls will return to the *status quo ante*. Journalists covering the Olympic games would do

well to come prepared with a reliable circumvention method and a list of banned Chinese language websites to check for accessibility.

Censorship circumvention

Given the matrix of controls, and the climate of self-censorship it engenders, it is difficult to determine how effective the system of censorship is in preventing people from accessing and posting information. Generally speaking, citizens are very reluctant to openly challenge the system or discuss circumvention methods. Although polling in an authoritarian regime is unreliable, some surveys indicate that a large proportion of Chinese people have little interest in evading government censorship, and may even support the Great Firewall. But such claims are difficult to believe in light of the lack of transparency, and the general climate of fear and suspicion within China. While the Internet is expanding dramatically, with a vibrant culture around social networking platforms, political discussions are noticeably absent from public forums, which are clouded with suspicions and reminders of state surveillance. And one of the most perverse aspects of censorship wherever it may occur is that citizens have no idea what they are missing if they have no idea it is being withheld in the first place, as is often the case in China.

There are nonetheless a wide variety of tools and methods that citizens can and do use to evade content filters in China ranging from the very simple to the complex. The Citizen Lab's recent publication, *Everyone's Guide to By-Passing Internet Censorship for Citizens Worldwide*, gives a comprehensive overview of these methods.[5] For example, DNS tampering and keyword methods described above can be easily circumvented by entering in the numerical IP address of the website instead. When the website of the Canadian Broadcasting Corporation (CBC) was filtered in China, our researchers determined that www.cbc.ca was being treated as a banned keyword; entering in the IP address for the site instead provided full access. There are numerous proxy and anonymizer websites and services that are employed but these can be technically challenging, insecure, slow, and unreliable. For example, it is very common for proxy computers to be set up outside China and their connection information broadcast in some manner (e.g., over radio or through public email lists) to Chinese citizens. However, many of these services are unencrypted and so easily monitored, and are set up by providers who are not personally known or trusted by the users, leaving the latter vulnerable to security forces. Additionally, they tend to be eventually placed on block lists by authorities, making them frustrating to use.

The Citizen Lab's circumvention software, psiphon, is employed within private social networks of trust. Citizens outside of censored jurisdictions set up

---

[5] Retrieved May 29, 2008 from http://www.civisec.org/guides-print.html

psiphon nodes on their home or office computers and then give the connection information privately to a few trusted friends, colleagues or family members. Since the connections between psiphon nodes and users are private and encrypted, and each psiphon node is separate from another, it is very difficult for authorities to track down and block. Moreover, unlike some other circumvention tools, psiphon requires no download on the client side, making it easy to use in multiple locations and safe in case authorities seize a computer. The psiphon team has begun work on a new version of the service that is entirely web-based, meaning psiphon node operators need not download any software in order to set up a node for their own private social network; the psiphon service takes care of that for them. Even citizens within censored countries like China can potentially start up their own nodes through the new web-based service. We have started testing the development version of this service with the help of our own network of trusted contacts within and outside China and the reports have been very positive so far.

Corporate Complicity

With now the world's largest number of Internet users, there is an enormous market opportunity for Internet services and equipment in China and corporations from around the world have sought to gain a toehold. Doing so requires many difficult compromises, as authorities seek to control their services to make sure they are consistent with government filtering policy, or even seek to enlist their help to maintain and extend it. As my ONI colleagues from Harvard Law School, John Palfrey and Colin Maclay, noted in their testimony before Congress on May 20, 2008, these pressures put corporations in a difficult quandary.[6] Compliance with local government policies can generate intense public criticism at home, shareholder activism, lawsuits and fines. Choosing not to comply can mean the withholding of market opportunities, contracts, and licenses, frivolous lawsuits and harassment, filtering and network tampering, and even public safety concerns for employees.

A number of US-based and Western high tech firms have thus chosen to comply with and thus aid Chinese censorship practices while finding various ways to try to contain and mitigate criticism back home. The US-based service companies Yahoo!, Microsoft, and Google, for example, have all engaged in various forms of self-censorship of their services in order to comply with local Chinese laws and regulations. These include the removal of contentious search terms from search engine results, deletion of offending posts, terms, and other

---

[6] Written Statement of John G. Palfrey, Jr. Clinical Professor of Law & Executive Director Berkman Center for Internet & Society, Harvard Law School with Colin Maclay Managing Director Berkman Center for Internet & Society, Harvard Law School May 20, 2008. Retrieved May 29, 2008 from http://blogs.law.harvard.edu/palfrey/2008/05/20/testimony-on-internet-filtering-and-surveillance/

entries from services, and, in at least one egregious case involving Yahoo!, the disclosure to the Chinese State Security Bureau of confidential user information leading to the arrest and sentencing to 10 years in prison of journalist Shi Tao.

Typically and not surprisingly, the corporations have been less than forthcoming about the specific compromises they make in order to do business in China. Some appear to have been deceitful. For example, a recently leaked Cisco presentation from 2002 showed that company members viewed China's then emerging censorship system (the so-called "Golden Shield") as a market opportunity, thus contradicting repeated claims made by the company that it is not morally responsible for sales of its equipment to regimes that censor and engage in surveillance. My colleague at the Citizen Lab, Senior Research Fellow and PhD candidate Nart Villeneuve, has just completed an exhaustive comparative analysis of the censorship practices of the search engines provided by Google, Microsoft and Yahoo! for the Chinese market, along with the domestic Chinese search engine Baidu.[7] Villeneuve's tests shows that each of the search engines removes an extensive set of politically sensitive information, including the web sites of Chinese dissidents and the Falun Gong movement, the web sites of major news organizations, such as the BBC, as well as international advocacy organizations, such as Human Rights Watch. His analysis also strongly suggests that because of a lack of consistency of blocked content across each search engine tested that the companies themselves are selecting the specific web sites to be censored, as opposed to being given a list by the Chinese government. Such self-selection raises the prospect of anticipatory over-blocking, in which content not officially blocked by China ends up being filtered because of the eagerness of search engines. Lastly, all of the search engines exhibited poor levels of user notification and transparency, with the level of overall transparency of Microsoft and Yahoo! actually declining over the last two years. Google's level of transparency has remained the same, but it is noteworthy that it has not improved at all during that time either.

Recommendations

(1) Encourage and Support the Multi-Stakeholder Initiative to Protect and Promote Privacy and Free Expression Worldwide

Several of my ONI colleagues at the Berkman Center for Internet and Society at Harvard University, along with Business for Social Responsibility, the Center for Democracy and Technology, companies and human rights groups have been involved in a multi-stakeholder initiative to protect and promote privacy and free expression worldwide. This initiative is designed to allow US companies a

---

[7] Nart Villeneuve, *Search Monitor Project: Toward a Measure of Transparency*, Citizen Lab Occasional Paper #1 (June 2008). Retrieved June 1, 2008 from http://www.citizenlab.org/papers/searchmonitor.pdf

chance to discuss the challenges described above while working towards a code of conduct that protects human rights. It takes place under the shadow of looming legislative measures, the Global Online Freedom Act (GOFA), currently under active consideration by Congress that would specify requirements and put forth serious penalties for companies who violate them.

In their testimony to Congress, my colleagues John Palfrey and Colin Maclay put forth several reservations to GOFA that have been echoed by other observers. I share these concerns. At present, I believe the most effective measure the US government can take is to facilitate widespread engagement with the multi-stakeholder initiative to ensure that meaningful participation and dialogue takes place among all those affected. At the same time, industry self-regulation can only be successful if significant changes occur and corporate practices evolve towards desirable ends. As Villeneuve's research shows, however, two of the three search engines involved in the multi-stakeholder initiative have actually become *less* transparent with respect to their filtering policies and practices in China, and none have improved.

(2) Support Independent Monitoring Efforts, such as those of the ONI and others.

The activities of the ONI have grown now to encompass nearly 100 researchers and the participation of several respected international NGOs. Recently, the International Development Research Centre (IDRC) of Canada has supported a new subsidiary project called ONI Asia that will involve 15 stakeholders throughout the Asia region who will actively participate in ONI research. The monitoring efforts of groups like the ONI are essential in order to provide an unbiased and empirically grounded picture of state censorship, surveillance, and information warfare practices around the world. They are also critical to multi-stakeholder initiatives as they give an independent audit of search engine and other companies' compliance with their own public pledges and thus prevent backsliding. Congress can encourage and support the research of the ONI, and others like it, in order to provide an accurate picture of the present nature of threats to freedom of speech, privacy, and access to information.

(3) Support Continued R &D and User Empowerment

According to the results of the ONI's last comparative study, there are now at least 26 countries that engage in some level of content filtering and perhaps many more yet to be documented. These developments shatter the long-standing myth that governments are powerless to control information flowing through the Internet. At the same time, many grassroots software tools have been developed that have empowered users to evade government censors, protect their privacy online, and exercise freedom of speech. However, most of the projects lack the financial and technical support needed to sustain them

over time. Many have become obsolete or insecure as a result. Our tool, psiphon, was developed in a University laboratory with a very small amount of funding from the Open Society Institute. The US government, along with other governments, international organizations, and foundations, can offer financial and other incentives, including facilitating training, education, outreach, and support for the development and dissemination of such tools as a way for citizens to safely and securely evade unlawful censorship and surveillance. Ultimately, empowering users to build and deploy technologies that support, rather than detract from, human rights is the most effective and immediate way to end Internet censorship worldwide.

(4) Initiate a Global Multilateral Effort to Address Internet Censorship Concerns and 'Protect the Net'

The concerns raised above about China's Internet content filtering practices are magnified by the fact of China's growing global economic and political clout. As an emerging regional telecommunications power, for example, there is a prospect that if left unaddressed China's censorship practices could be "exported" to neighboring or allied countries as a consequence of connectivity or services acquired through or from China. Furthermore, China's domestic policies could legitimize Internet content filtering practices as the norm for other countries to follow elsewhere unless they are specifically countered in international settings. Most illustrative of this tension is the question of China's use of "offensive" blocking techniques (such as DDOS attacks), which can be construed as a violation of international law. Left unchallenged, however, such techniques can become a de facto global norm making it "fair game" for governments to take down critical voices online wherever those may be located.

All of these concerns point to the value and urgency of the US government initiating a global multilateral, multi-stakeholder effort to address freedom of speech, access to information and privacy online – to, in effect, lead the effort worldwide to *protect the net*. However, such efforts will require consistency of US policy in this area, both domestically and internationally. While the efforts of this Commission and others like it are laudable (I am unaware of such a commission taking place in Canada, for example, in spite of the involvement of Canadian companies in the Chinese information security market), far too often attention is paid to violators of human rights that happen to be adversaries of the United States, such as Iran and China, while other countries with similar policies allied to the United States escape censure. Likewise, criticism of China's vast censorship, surveillance, and infowar practices rings hollow in light of revelations of extra-legal surveillance of the Internet occurring in the United States itself, or US military development of information warfare techniques that propose to "fight and win wars in cyberspace." Echoing the comments made by my colleagues John Palfrey and Colin Maclay, the US government needs to show the way by examining its own domestic and foreign policies with respect

to data retention, surveillance and information warfare. Only then will criticism directed towards China and other countries like it carry the full moral weight it presently lacks.