Testimony by
Rebecca MacKinnon
Visiting Fellow, Center for Information Technology Policy,
Princeton University

at the hearing:
"China, the Internet, and Google"
Congressional-Executive Commission on China
March 1, 2010

Thank you, Mr. Chairman, for giving me the opportunity to testify today. I am Rebecca MacKinnon, a visiting fellow at Princeton University's Center for Technology Policy. From 1992-2001, for more than nine years, I worked as a journalist for CNN in China. For the last six years while based at several different academic institutions I have researched Chinese Internet censorship alongside global censorship trends, examining in particular how the private sector assists government efforts to silence or manipulate citizen speech. I am a founding member of the Global Network Initiative, a non-governmental multi-stakeholder initiative that aims to help Internet and telecommunications companies uphold the principles of free expression and privacy around the world. I am also co-founder of an international bloggers' network called Global Voices Online. Several of our contributors regularly summarize and translate conversations from the Chinese blogosphere, and report on developments related to online free expression in China. My testimony today is informed by my experience as a journalist who has lived under Chinese censorship and surveillance; as a researcher of Chinese Internet censorship; as a practitioner of new media and participant in Chinese-language online communities; and as an advocate for free expression and human rights on the Internet.

On January 12th Google stunned the world with its dramatic announcement that it was reconsidering its business in China in the wake of debilitating cyber-attacks, and furthermore that the company was no longer willing to continue operating a censored search engine in China, Google.cn, launched in January 2006.[1] In my testimony, I will briefly describe the context of the Google announcement. I will then outline some of the different tactics used by the Chinese government to censor and control online speech, including tactics used against Google. I will describe what some Chinese citizens are doing in order to evade and oppose these tactics. Finally, I will offer some specific policy suggestions for how the United States can help to improve Internet freedom in China.

The context of Google's China announcement

American Internet company executives have long argued that more connectivity will bring more freedom - even in repressive regimes where the Internet is under heavy censorship and surveillance. Statements to that effect were a common theme in Congressional testimony given by Google and Yahoo executives at the February 2006

[1] *A new approach to China*, by David Drummond,The Official Google Blog, Jan. 12, 2010, at: http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

hearing convened by the late Rep. Tom Lantos.[2] Since then, Chinese Internet usage has nearly quadrupled. Stories abound of how Internet users in China have helped expose corruption, bring justice to innocent victims of official malfeasance, and even change some laws and regulations. But this has not changed the regime's repressive attitude toward dissent. According to a recent report by the Dui Hua Foundation, in 2008 arrests and indictments on charges of "endangering state security" – the most common charge used in cases of political, religious, or ethnic dissent – more than doubled for the second time in three years.[3]

China is pioneering a new kind of Internet-age authoritarianism. It is demonstrating how a non-democratic government can stay in power while simultaneously expanding domestic Internet and mobile phone use. In China today there is a lot more give-and-take between government and citizens than in the pre-Internet age, and this helps bolster the regime's legitimacy with many Chinese Internet users who feel that they have a new channel for public discourse. Yet on the other hand, as this Commission's 2009 Annual Report clearly outlined, Communist Party control over the bureaucracy and courts has strengthened over the past decade, while the regime's institutional commitments to protect the universal rights and freedoms of all its citizens have weakened.[4]

Google's public complaint about Chinese cyber-attacks and censorship occurred against this backdrop. It reflects a recognition that China's *status quo* – at least when it comes to censorship, regulation, and manipulation of the Internet – is unlikely to improve any time soon, and may in fact continue to get worse.

Overview of Chinese Internet controls

Chinese government attempts to control online speech began in the late 1990's with a focus on the filtering or "blocking" of Internet content. Today, the government deploys an expanding repertoire of tactics. They include: deletion or removal of content at the source, device and local-level controls, domain name controls, localized disconnection or restriction, self-censorship due to surveillance, cyber-attacks, government "astro-turfing," local government "outreach," and targeted police intimidation.

---

[2] Testimony of Google Inc. before the Subcommittee on Asia and the Pacific, and the Subcommittee on Africa, Global Human Rights, and International Operations, Committee on International Relations, United States House of Representatives, February 15, 2006, by Elliot Schrage, Vice President, Global Communications and Public Affairs, Google Inc., at: http://googleblog.blogspot.com/2006/02/testimony-internet-in-china.html; and Testimony of Michael Callahan, Senior Vice President and General Counsel, Yahoo! Inc., Before the Subcommittees on Africa, Global Human Rights and International Operations, and Asia and the Pacific, February 15, 2006, at: http://yhoo.client.shareholder.com/press/ReleaseDetail.cfm?ReleaseID=187725

[3] "Chinese State Security Arrests, Indictments Doubled in 2008," *Dui Hua Human Rights Journal*, March 25, 2009, at: http://www.duihua.org/hrjournal/2009/03/chinese-state-security-arrests.html

[4] 2009 Annual Report, Congressional-Executive Commission on China, at: http://www.cecc.gov/pages/annualRpt/annualRpt09/CECCannRpt2009.pdf

- **Filtering or "blocking:"** This is the original and best understood form of Internet censorship. Internet users on a particular network are blocked from accessing specific websites. The technical term for this kind of censorship is "filtering." Some congressional proceedings and legislation have also referred to this kind of censorship as "Internet jamming." Filtering can range in scope from a home network, a school network, university network, corporate network, the entire service of a particular commercial Internet Service Provider (ISP), or all Internet connections within a specific country. It is called "filtering" because a network administrator uses special software or hardware to block access to specified web pages by banning access to certain designated domain names, Internet addresses, or any page containing specified keywords or phrases. A wide range of commercial filtering products are developed and marketed here in the United States by U.S. companies for filtering by parents, schools, government departments, businesses, and anybody else who wants to control how their networks are used. All Internet routers – including those manufactured by the U.S. company Cisco Systems – come with the ability to filter because it is necessary for basic cyber-security and blocking universally reviled content like child pornography. However, the same technology can just as easily be used to block political content. According to the Open Net Initiative (ONI), an academic consortium that has been following global Internet filtering since 2002, more than forty countries now practice Internet filtering to some extent at the national level. However China's Internet filtering system – known to many as "the Great Firewall of China" – is the most sophisticated and extensive in the world.[5] In its 2009 report on Chinese Internet censorship, the ONI described increasingly pervasive and sophisticated filtering tactics. "In fine-tuning this system," the report concluded, "China is also adopting subtler and more fluid controls."[6]

- **Deletion and removal of content:** Filtering is the primary means of censoring content over which the Chinese government has no jurisdiction. When it comes to websites and Internet services over which Chinese authorities do have legal jurisdiction – usually because at least some of the company's operations and computer servers are located in-country – why merely block or filter content when you can delete it from the Internet entirely? In Anglo-European legal parlance, the legal mechanism used to implement such a system is called "intermediary liability." The Chinese government calls it "self-discipline," but it amounts to the same thing, and it is precisely the legal mechanism through which Google's Chinese search engine, Google.cn, was required to censor its search results.[7] All

---

[5] See *Access Denied: The Practice and Policy of Global Internet Filtering* by Diebert, et.al. (MIT Press, 2008). Updates and new country reports are posted regularly at the Open Net Initiative website at: http://opennet.net

[6] "China" research profile by Stephanie Wang, Open Net Initiative, published on June 15, 2009 at: http://opennet.net/research/profiles/china

[7] See *Race To the Bottom: Corporate Complicity in Chinese Internet Censorship* by Human Rights Watch (August 2006), at http://www.hrw.org/reports/2006/china0806/. Also "Search Monitor Project: Toward a Measure of Transparency," by Nart Villeneuve, Citizen Lab

Internet companies operating within Chinese jurisdiction – domestic or foreign – are held liable for everything appearing on their search engines, blogging platforms, and social networking services. They are also legally responsible for everything their users discuss or organize through chat clients and messaging services. In this way, much of the censorship and surveillance work is delegated and outsourced by the government to the private sector – who, if they fail to censor and monitor their users to the government's satisfaction, will lose their business license and be forced to shut down. It is also the mechanism through which China-based companies must monitor and censor the conversations of more than fifty million Chinese bloggers. Politically sensitive postings are deleted or blocked from ever being published. Bloggers who get too influential in the wrong ways can have their accounts shut down and their entire blogs erased. That work is done primarily not by "Internet police" but by employees of Internet companies.[8]

- **Cyber-attacks:** The sophisticated, military-grade cyber-attacks launched against Google were targeted specifically at GMail accounts of human rights activists who are either from China or work on China-related issues. This serves as an important reminder that governments and corporations are not the only victims of cyber-warfare and cyber-espionage. Human rights activists, whistleblowers and dissidents around the world, most of whom lack training or resources to protect themselves, have over the past few years been victim of increasingly aggressive cyber attacks.[9] The effect in some cases is either to bring down overseas dissident websites at critical political moments, or causing frequent outages, putting great strain on the site's operators just to keep it running. Websites run by Chinese exiles, dissidents, and human rights defenders have seen increasingly aggressive attacks over the past few years.[10] In other cases the effect is to compromise activists' internal computer networks and e-mail accounts to the point that it becomes too risky to use the Internet at all for certain kinds of organizing and communications, because the dissidents don't feel confident that any of their digital communications are secure. Journalists who report on human rights issues and academics whose research includes human rights problems have also found themselves under aggressive attack in places like China, exposing their sources and making it much more risky to work on politically sensitive topics. Like the

---

Occasional Paper, No.1, University of Toronto (June 2008) at http://www.citizenlab.org/papers/searchmonitor.pdf

[8] For more details see "China's Censorship 2.0: How companies censor bloggers," by Rebecca MacKinnon, *First Monday* (February 2006) at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089; and "The Chinese Censorship Foreigners Don't See," by Rebecca MacKinnon, *The Wall Street Journal Asia*, August 14, 2008, at: http://online.wsj.com/article/SB121865176983837575.html

[9] See *Tracking Ghostnet: Investigating a Cyber Espionage Network*, by Information War Monitor (March 2009) at http://www.nartv.org/mirror/ghostnet.pdf

[10] "Chinese human rights sites hit by DDoS attack," by Owen Fletcher, *ComputerWorld*, January 26, 2010, at: http://www.computerworld.in/articles/chinese-human-rights-sites-hit-ddos-attack

activists, these groups are unprepared and unequipped to deal with cyber-attacks.[11]

- **Device-level and local controls:** In late spring of 2009 the Ministry of Industry and Information Technology (MIIT) mandated that by July 1st of that year all computers sold in China must be pre-installed with a specific software product called "Green Dam – Youth Escort."[12] While the purpose of "Green Dam" was ostensibly for child protection, researchers inside and outside of China quickly uncovered the fact that it not only censored additional political and religious content, it also logged user activity and sent this information back to a central computer server belonging to the software developer's company.[13] The software had other problems which made it easy for U.S. industry to oppose: It contained serious programming flaws which increased the user's vulnerability to cyber-attack. It also violated the intellectual property rights of a U.S. company's filtering product. Faced with uniform opposition from the U.S. computer industry and strong protests from the U.S. government, the MIIT backed down on the eve of its deadline, making the installation of Green Dam voluntary instead of mandatory.[14] The defeat of Green Dam, however, did not diminish other efforts to control and track Internet user behavior at more localized levels within the national "Great Firewall" system – for instance at the level of a school, university, or apartment block as well as at the level of a city-wide Internet Service Provider (ISP). It was reported in September last year that local governments were mandating the use of censoring and surveillance products with names like "Blue Shield" and "Huadun." The function and purpose of these products appeared similar to Green Dam, though they had the benefit of involving neither the end user nor foreign companies.[15] The implementation of these systems has received little attention outside of China.

---

[11] "National Day triggers censorship, cyber attacks in China," Committee to Protect Journalists, September 22, 2009 at: http://cpj.org/2009/09/national-day-triggers-censorship-cyber-attacks-in.php

[12] "China Squeezes PC Makers," by Loretta Chao, *The Wall Street Journal*, June 8, 2009, at: http://online.wsj.com/article/SB124440211524192081.html

[13] *China's Green Dam: The Implications of Government Control Encroaching on the Home PC*, Open Net Initiative bulletin (June, 2009) at: http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc; *Analysis of the Green Dam Censorware System*, by Scott Wolchok, Randy Yao, and J. Alex Halderman, Computer Science and Engineering Division, The University of Michigan, June 11, 2009, at: http://www.cse.umich.edu/%7Ejhalderm/pub/gd/.

[14] "After the Green Dam Victory," by Rebecca MacKinnon, *CSIS Freeman Report*, June/July 2009, at: http://csis.org/files/publication/fr09n0607.pdf

[15] "China Clamps Down on Internet Ahead of 60th Anniversary," by Owen Fletcher, IDG News Service, September 25, 2009 at: http://www.pcworld.com/article/172627/china_clamps_down_on_internet_ahead_of_60th_anniversary.html ; and "China: Blue Dam activated," by Oiwan Lam, *Global Voices Advocacy*, September 13, 2009 at: http://advocacy.globalvoicesonline.org/2009/09/13/china-blue-dam-activated/

- **Domain name controls:** In December, the government-affiliated China Internet Network Information Center (CNNIC) announced that it would no longer allow individuals to register Internet domain names ending in .cn. Only companies or organizations would be able to use the .cn domain.[16] While authorities explained that this measure was aimed at cleaning up pornography, fraud, and spam, a group of Chinese webmasters protested that it also violated individual rights.[17] Authorities announced that more than 130,000 websites had shut down in the cleanup. In January a Chinese newspaper reported that self-employed individuals and freelancers conducting online business had been badly hurt by the measure.[18] Later in February, CNNIC backtracked somewhat, announcing that individuals will once again be allowed to register .cn domains, but all applicants must appear in person to confirm their registration, show a government ID, and submit a photo of themselves with their application. [19] This eliminates the possibility of anonymous domain name registration under .cn and makes it easier for authorities to warn or intimidate website operators when "objectionable" content appears.

- **Localized disconnection and restriction:** In times of crisis when the government wants to ensure that people cannot use the Internet or mobile phones to organize protests, connections are shut down entirely or heavily restricted in specific locations. There have been anecdotal reports of Internet connections going down or text-messaging services suddenly not working in counties or towns immediately after local disturbances broke out. The most extreme case however is Xinjiang province, a traditionally Muslim region bordering Pakistan, Kazakhstan, and Afghanistan in China's far Northwest. After ethnic riots took place in July of last year, the Internet was cut off in the entire province for six months, along with most mobile text messaging and international phone service. Nobody in Xinjiang could send e-mail or access any website – domestic or foreign. Businesspeople had to travel to the bordering province of Gansu just to communicate with customers.[20] Internet access and phone service have now been restored, but with severe limitations on the number of text messages people can send on their mobile phones per day, no access to overseas websites, and even very limited access to

---

[16] "China tightens control on domain name registration," by Zhao Chunzhe, China Daily, December 14, 2009, at: http://www.chinadaily.com.cn/china/2009-12/14/content_9174767.htm

[17] "China: Online protest against CNNIC," by Oiwan Lam, *Global Voices Advocacy*, December 22, 2009 at: http://advocacy.globalvoicesonline.org/2009/12/22/china-online-protest-against-cnnic/

[18] "China: More than 100 thousand websites shut down," by Oiwan Lam, *Global Voices Advocacy*, February 3, 2010, at: http://advocacy.globalvoicesonline.org/2010/02/03/china-more-than-100-thousand-websites-shut-down/

[19] "China Further Tightens Rules for Domain Name Owners," by Owen Fletcher, PCWorld, February 23, 2010, at: http://www.pcworld.com/article/190013/china_further_tightens_rules_for_domain_name_owners.html

[20] "What Internet? China region cut off 6 months now," by Cara Anna, Associated Press via Yahoo! News, January 19, 2010, at: http://news.yahoo.com/s/ap/20100119/ap_on_bi_ge/as_china_internet_blackout

domestic Chinese websites. Xinjiang-based Internet users can only access specially watered-down versions of official Chinese news and information sites, with many of the functions such as blogging or comments disabled.[21]

- **Self-censorship due to surveillance:** Surveillance of Internet and mobile users is conducted in a variety of ways, contributing to an atmosphere of self-censorship. Surveillance enables authorities to warn and harass Internet users either via electronic communications or in person when individuals are deemed to be taking their online activities too far. Occasional detention, arrest, or imprisonment of select individuals serves as an effective warning to others that they are being watched. Surveillance techniques include:

    - *"Classic" monitoring:* While Chinese surveillance measures are explained by the government to the public as anti-terrorism measures, they are also broadly used to identify, then harass or imprison peaceful critics of the regime. Cybercafes – the cheaper and more popular option for students and less affluent people – are required to monitor users in multiple ways including ID registration upon entry to the café or upon login, surveillance cameras, and monitoring software installed on computers. Surveillance in Chinese cybercafes is known to be so extensive that people who are likely to engage in political conversations online avoid doing so in such facilities.

    - *"Law enforcement compliance:"* In a country like China where "crime" is defined broadly to include political dissent, companies with in-country operations and user data stored locally can easily find themselves complicit in the surveillance and jailing of political dissidents. The most notorious example of law enforcement compliance gone badly wrong was when Yahoo's local Beijing staff gave Chinese police account information of journalist Shi Tao, activist Wang Xiaoning, and at least two others engaged in political dissent.[22] There are other examples of how law enforcement compliance by foreign companies has compromised activists. In 2006, Skype partnered with a Chinese company to provide a localized version of its service, then found itself being used by Chinese authorities to track and log politically sensitive chat sessions by users inside China.[23] This happened because Skype delegated law enforcement compliance to its local partner without sufficient attention to how the compliance was being carried out. China's more sophisticated and politically aware

[21] "Blogger describes Xinjiang as an 'internet prison'," Josh Karamay, BBC News, February 3, 2010, at: http://news.bbc.co.uk/2/hi/asia-pacific/8492224.stm

[22] For detailed analysis of the Yahoo! China case see "Shi Tao, Yahoo!, and the lessons for corporate social responsibility," working paper presented at presented December 2007 at the International Conference on Information Technology and Social Responsibility, Chinese University, Hong Kong, at: http://rconversation.blogs.com/YahooShiTaoLessons.pdf

[23] *Breaching Trust*, by Nart Villeneuve, Information Warfare Monitor and ONI Asia Joint Report (October 2008), at: http://www.nartv.org/mirror/breachingtrust.pdf

Internet users have long assumed that Chinese-branded e-mail and chat services monitor their communications and share them readily with authorities. As news about these incidents involving foreign-branded products spread among Chinese Internet users, however, many no longer feel that they can trust foreign brands either. They feel they have no choice but to minimize the extent to which they use any Internet or mobile service for politically sensitive conversations for fear that anything and everything might be compromised.

- **Pro-active measures: "astro-turfing" and outreach:** The government increasingly combines censorship and surveillance measures with pro-active efforts to steer online conversations in the direction it prefers. In 2008 the Hong Kong-based researcher David Bandurski determined that at least 280,000 people had been hired at various levels of government to work as "online commentators." Known derisively as the "fifty cent party," these people are paid to write postings that show their employers in a favorable light in online chat rooms, social networking services, blogs, and comments sections of news websites.[24] Many more people do similar work as volunteers – recruited from among the ranks of retired officials as well as college students in the Communist Youth League who aspire to become Party members. This approach is similar to a tactic known as "astro-turfing" in American parlance, now commonly used by commercial advertising firms, public relations companies, and election campaigns around the world.[25] In many provinces it is now also standard practice for government officials – particularly at the city and county level – to work to co-opt and influence independent online writers by throwing special conferences for local bloggers, or inviting them to special press events or news conferences about issues of local concern.[26]

All of these measures are implemented in the context of the Chinese government's broader policies on information and news control. In December the Committee to Protect Journalists listed China as the world's top jailer of journalists.[27]

---

[24] "China's Guerilla War for the Web," by David Bandurski, *Far Eastern Economic Review*, July 2008, at: http://www.feer.com/essays/2008/august/chinas-guerrilla-war-for-the-web

[25] "Astroturfing describes the posting of supposedly independent messages on Internet boards by interested companies and individuals In American politics, the term is used to describe formal public relations projects which deliberately give the impression that they are spontaneous and populist reactions. The term comes from AstroTurf -- the fake grass used in many indoor American football stadiums. The contrast between truly spontaneous or "grassroots" efforts and an orchestrated public relations campaign, is much like the distinction between real grass and AstroTurf." From http://www.answers.com/topic/astroturfing

[26] "How China polices the internet," by Kathrin Hille, *Financial Times*, July 17, 2009 at: http://www.ft.com/cms/s/2/e716cfc6-71a1-11de-a821-00144feabdc0.html

[27] "2009 Prison Census," Committee to Protect Journalists, (as of December 1, 2009) at: http://cpj.org/imprisoned/2009.php

Citizen pushback

Despite the government's formidable array of control tactics, China's determined, creative, and opinionated Internet users have managed to make the Chinese Internet a lively, fun, and often contentious place.[28] Over the past six years I have been involved with a number of Chinese blogger groups, mailing lists, and social networks. Chinese "netizens" – as they call themselves – are doing a range of things to oppose Internet controls:

- **Informal anti-censorship support networks:** I have attended gatherings of bloggers and journalists in China – with varying degrees of organization or spontaneousness – where participants devoted significant amounts of time to teaching one another how to use circumvention tools to access blocked websites. Informal "teach-ins" on how to access Twitter are especially popular among people who want access to an uncensored, international community of conversation. Certain bloggers are known to post information about how to circumvent censorship and welcome their friends to copy and re-post their work as widely as possible. I have seen numerous Powerpoints presentations and PDF documents containing instruction manuals on how to use various tools, circulated by e-mail or through peer-to-peer instant messaging clients.

- **Distributed web-hosting assistance networks:** I am aware of people who have strong English language and technical skills, as well as overseas credit cards, who are helping friends and acquaintances in China to purchase inexpensive space on overseas web hosting services, then set up independent blogs using free open-source software. The objective is to help people who don't have the technical skills to run a website on their own to avoid a) being victim of content removal if they use domestic services, or b) being blocked if they use popular international blogging platforms like Blogspot, Typepad, Livejournal, or Wordpress.com, all of which are blocked in China. Sometimes the people doing this largely volunteer work also help bloggers to switch domain names and IP addresses when the blog gains attention and gets blocked by the "great firewall."

- **Crowdsourced "opposition research:"** With the Chinese government's Green Dam censorware edict last year, we have seen the emergence of loosely organized "opposition research" networks. Last June a group of Chinese computer programmers and bloggers collectively wrote a report exposing Green Dam's political and religious censorship, along with many of its security flaws. They posted the document at Wikileaks.[29] Another anonymous group of Chinese

---

[28] For an excellent portrayal of Chinese Internet culture and its contentious, playful nature see *The Power of the Internet in China: Citizen Activism Online* by Guobin Yang, (Columbia University Press, 2009).

[29] "A technical analysis of the Chinese "Green Dam Youth Escort" censorship software," posted June 2009 on Wikileaks.org at: http://wikileaks.org/wiki/A_technical_analysis_of_the_Chinese_%27Green_Dam_Youth-

netizens have collected a list of companies and organizations – domestic and foreign – who have helped build China's Internet censorship system.[30]

- **Preservation and relay of censored content:** I have noticed a number of people around the Chinese blogosphere and in chatrooms who make a regular habit of immediately downloading interesting articles, pictures, and videos which they think have a chance of being blocked or removed. They then re-post these materials in a variety of places, and relay them to friends through social networks and e-mail lists.

- **Humorous "viral" protests:** In 2009, Internet censorship tightened considerably. Many lively blogging platforms and social networks where heated political discussions were known to take place were shut down under the guise of an anti-porn crackdown. In response, an anonymous Shanghai-based jokester created an online music video called "Ode to the Grass Mud Horse" – whose technically innocent lyrics, sung by a children's chorus over video of alpaca sheep, contained a string of highly obscene homonyms. The video spawned an entire genre of anti-censorship jokes and videos involving mythical animals whose names sound similar to official slogans and obscenities of various kinds.[31] This viral pranksterism created an outlet for people to vent about censorship, poke fun at the government, and raise awareness among many people who are not comfortable discussing such matters in a direct way.

- **Public persuasion efforts:** A number of prominent liberal Chinese intellectuals and journalists occasionally write essays on personal blogs in which they criticize the government's censorship and information control policies as counterproductive: censorship, they argue, stifles the Chinese people's innovation and creativity, contributes to corruption and economic inefficiency, and generally prevents the nation from fulfilling its real potential. Such arguments have failed to influence government policies in any kind of meaningful way, although individual officials and business leaders sometimes do echo these sentiments in public fora.[32] It remains unclear when or whether this line of argument will eventually convince China's leadership to relax information controls. The good news, however, is that in China today it is at least possible to make this argument.

Escort%27_censorship_software (At time of writing the page cannot be reached due to bandwith and funding problems at Wikileaks.org)

[30] "GFW Engineering Team Name List," posted to Google Documents in January 2010 at: http://docs.google.com/View?docid=0Ae8NBXfKeGvqZGR0am1yeGRfMWhyZDljcWY4

[31] "A Dirty Pun Tweaks China's Online Censors," by Michael Wines, *The New York Times*, March 11, 2009, at: http://www.nytimes.com/2009/03/12/world/asia/12beast.html

[32] "Charles Zhang: Without Reform There is No Way Out" by Xiao Qiang, *China Digital Times,* February 4, 2010, at: http://chinadigitaltimes.net/2010/02/charles-zhang-%E5%BC%A0%E6%9C%9D%E9%98%B3%EF%BC%9Awithout-reform-there-is-no-way-out/

Recommendations

Because the Chinese government deploys an expanding range of tactics to control online speech, efforts to promote Internet freedom in China should be similarly multi-pronged and multi-faceted. China's Internet users are pushing back against the controls in a range of ways, as I have described. It is thus important to support, encourage, and enable a range of efforts aimed at tackling different parts of the problem. Finally, corporate social responsibility is essential: It will be much more difficult for Chinese Internet users to fight for their rights if the international business community assists the Chinese government in finding more effective means to muzzle them.

- **Anti-censorship tools:** Congress is to be commended for giving both moral and financial support to programmers who are working hard to develop anti-censorship technologies. In spite of this, I have never ceased to be amazed by the number of university students, academics, journalists, and other white-collar professionals I've encountered on frequent trips to China over the past few years who profess little or no knowledge of circumvention tools and techniques. While no survey data exists to shed light on what percentage of Chinese Internet users know how to circumvent censorship – or are interested in doing so even if they know how – the anecdotal evidence I have gathered leads me to concluded that the percentage must be relatively small, and concentrated among elite groups of tech-savvy people who work in the Internet industry, followers of banned religious groups, and politically active people. The broader Internet-using public in China appears to be largely in the dark about how to access blocked websites. Funding for software development, therefore, needs to be accompanied by equally robust support for education and outreach among broader segments of Chinese society beyond the obvious communities.

- **Anonymity and security tools:** In my interactions with Chinese journalists, human rights, lawyers, bloggers, and academics, I've found that most of them are shockingly uneducated about how to evade online surveillance, how to secure their e-mail, how to detect and eliminate spyware on their computers, and how to guard against even the most elementary cyber-attacks. Chinese-language, culturally appropriate technologies, accompanied by robust education and training, is badly needed. The recent attacks against Chinese GMail users only highlights the urgency.

- **Capture, preservation, and distribution of censored content:** As I mentioned earlier, a lot of Chinese Internet users are downloading and preserving content before it gets censored, but in an ad-hoc and unorganized way. A searchable, accessible, and secure repository of such materials would be invaluable if somebody had the time, funds, and technical support to create one.

- **Support for "opposition research":** To date, ad-hoc groups conducting research aimed at exposing details of Chinese censorship policies rely primarily on two platforms to publish their findings: Google Documents and Wikileaks.org. It is

unclear whether Google Documents will remain accessible in China if Google shuts down Google.cn and reduces or closes its China operations. Wikileaks.org faces bandwith problems and financial difficulties resulting in frequent inaccessibility. Chinese opposition researchers could use help in finding secure, reliable, and accessible platforms through which their work can be disseminated.

- **Corporate responsibility:** To ensure that American Internet businesses in China assume the appropriate level of responsibility for the human rights of their users and customers, I support a voluntary component backed up by legislation if necessary.

    - *Global Network Initiative:* In 2008 Google, Yahoo, and Microsoft took the important step of joining the Global Network Initiative (GNI), a code of conduct for free expression and privacy for companies in the Information & Communications Technologies (ICT) sector.[33] The GNI can help companies uphold a shared commitment to the values of free expression and privacy while recognizing that no market is without political difficulties or ethical dilemmas. Just as companies have a social responsibility not to pollute the environment or exploit twelve-year-olds, American companies have a responsibility not to collaborate with the suppression of peaceful speech. The GNI's philosophy is grounded in the belief that people in all markets stand to benefit from Internet and mobile technologies. In most cases companies can still do a lot of good by being engaged in countries whose governments practice at least one of the forms of Internet controls I have described above – as long as they are aware of the human rights implications of their business and technical decisions. It is reasonable to expect all Internet and telecommunications companies to include human rights risk assessments in their decisions about market entry and product development, just as they and other companies consider environmental risks and labor concerns. With a multi-stakeholder membership including human rights groups, socially responsible investors and academics like myself, GNI's goal is to help companies do the right thing while bringing expanded Internet communications and mobile access to the people who stand to benefit from this connectivity the most.

      The principles' implementation guidelines and accountability framework can be adapted to a range of business models, including hardware companies and Internet service providers if these companies choose to engage with the GNI. As this Commission is aware, Senator Dick Durbin has written to thirty companies urging them to join the GNI and we look forward to working with them so that it will be possible for them to join in the near future. While GNI is presently most relevant to Yahoo, Google and Microsoft because those were the three companies that launched the initiative, it is also apparent that the thirty companies contacted by Senator

[33] See http://globalnetworkinitiative.org

Durbin share varying degrees of human rights risk, even as their business models, technologies, and geographies vary widely. They have an obligation to at least consider joining the GNI and if they choose not to, to find other appropriate policy and operational responses to address the inescapable human rights implications of their products or services.

- *Legislation* – While recognizing that no connectivity at all is even worse than censored connectivity, and also recognizing that many information communications technologies have "dual use" capabilities that can be used for security and legitimate law enforcement as well as repression, it should nonetheless be made more difficult for U.S. companies to provide censorship and surveillance capabilities to Chinese government entities and their corporate affiliates, given the regime's clear track record of using those technologies to suppress peaceful political dissent. It is important, however, that legislation be flexible enough to accommodate the rapidly-changing nature of information communications technology, as well as the complex and highly diverse nature of ICT businesses – including many small startups, as well as innovations that are difficult to define, categorize, or predict in advance. It is also important that any law concerning the human rights implications of ICTs be truly global in scope, recognizing that ICT companies can face human rights dilemmas in almost every market, whether the government involved is technically categorized as "democratic" or "authoritarian."

- *Legal support for victims:* Companies will have a further disincentive to collaborate with repressive surveillance and censorship if victims or corporate collaboration in human rights abuses can more easily sue them in a United States court of law.

- *Incentives for socially responsible innovation:* Companies should be encouraged to develop technologies and service features that enhance users' ability to evade censorship and surveillance, and to help users better understand what personal information is being stored and how it is used.

Conclusion:

Many of China's 384 million Internet users are engaged in passionate debates about their communities' problems, public policy concerns, and their nation's future. Unfortunately these public discussions are skewed, blinkered, and manipulated – thanks to political censorship and surveillance. The Chinese people are proud of their nation's achievements and generally reject critiques by outsiders even if they agree with some of them. A democratic alternative to China's Internet-age authoritarianism will only be viable if it is conceived and built by the Chinese people from within. In helping Chinese "netizens" conduct an un-manipulated and un-censored discourse about their future, the United States will not imposing its will on the Chinese people, but rather helping the Chinese people to take ownership over their own future.