Testimony of Rebecca MacKinnon
Visiting Fellow, Center for Information Technology Policy, Princeton University
Co-Founder, Global Voices Online (globalvoicesonline.org)

"The Google Predicament:
Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade"

Committee on Foreign Affairs
United States House of Representatives
February 10, 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. Earlier in my career I worked as a journalist for CNN in China for more than nine years. 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. In 2006 I became involved in discussions between members of industry, human rights groups, investors, and academics which eventually led to the formation in 2008 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, which is now five years old and has an active community of contributors from more than 100 countries. Several of our community members have been jailed or exiled because of their online activities, and many more have been threatened. My testimony today is informed by my experience as a journalist who has lived under authoritarian censorship and surveillance; as a researcher of Internet censorship; as a practitioner of new media; and as an advocate for free expression and human rights on the Internet.

Mr. Chairman, in my testimony today I will first present an overview of the major ways in which governments censor and monitor their citizens' online activities – often with private sector assistance. I will then offer a few specific policy recommendations, for companies as well as for government, on how the United States might work most effectively and constructively to promote, protect, and expand global Internet freedom.

Expanding techniques of authoritarian control

Over the past five years many authoritarian regimes have shifted from *reactive* to *proactive* in terms of how they deal with the Internet. Most modern authoritarian governments now accept the Internet as an irreversible reality. Rather than try to restrict citizens' access, the most proactive regimes are working aggressively to use Internet and mobile technologies to their own advantage.

In the course of my research I have found that while China has developed the most sophisticated system of Internet censorship and surveillance in the world, it has also

become the model for many other authoritarian governments that recognize the need to evolve and adapt in order to survive. It is no longer possible to be economically competitive without also being connected to the global Internet. At the same time regimes are finding flexible but effective ways to control and manipulate online speech and suppress citizen dissent – not controlling everybody and everything one hundred percent, but squashing or isolating certain types of Internet speech effectively enough that they can prevent opposition movements from succeeding, or in some cases even from emerging.

Last week Iran's chief of police summed up this approach in an interview with the Iranian official news agency, warning protestors against using e-mail, text messaging and social networks to organize demonstrations. "The new technologies allow us to identify conspirators and those who are violating the law without having to control all people individually," he said.[1] The Iranian government recently set up an official cyber defense command under the Islamic Revolutionary Guards Corps to fight "cyber crime" – with "crime" defined broadly to include criticism of the Ahmadinejad regime.[2]

Governments now use a range of technical, legal, commercial and political mechanisms to censor, manipulate, and monitor citizens' online speech. Below is a partial list:

- **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, 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.

---

[1] "Iran's police vow no tolerance towards protesters," Reuters, February 6, 2010 at http://www.reuters.com/article/idUSTRE61511N20100206

[2] "In Run-Up to Islamic Revolution Day 2010, Iranian Regime Steps Up Oversight, Censorship on Media, Citizens," *The Middle East Media Research Institute*, February 5, 2010 at: http://www.memri.org/report/en/0/0/0/0/0/0/3956.htm

China's Internet filtering system – known to many as "the Great Firewall of China" – is the most sophisticated and extensive in the world. Researchers believe Iran to have developed the world's second-most comprehensive system of filtering. But filtering is widely deployed on the national level in Asia, the Middle East, and increasingly though more narrowly in Europe.[3]

- **Removal and deletion:** Filtering is the primary means of censoring content over which an authority has no jurisdiction. When it comes to websites and Internet services over which a government does 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? The technical means for deleting content, or preventing its publication or transmission in the first place, vary depending on the country and situation. The legal mechanism, however, is essentially the same everywhere. In Anglo-European legal systems we call it "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.[4] All 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 in China 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 conversations are deleted or prevented from 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.[5]

---

[3] 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

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

[5] 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

- **Surveillance:** Surveillance of Internet and mobile phone users is conducted in a variety of ways. They include:

    - *"Classic" surveillance:* Egypt, named by the free expression group Reporters Without Borders as one of twelve "enemies of the Internet," engages in very little censorship and relies instead on surveillance – backed up by arrest, harassment, and torture – to keep online speech in check. [6] In Egypt and many other countries, heavy surveillance laws and regulations are called anti-terrorism measures, but they are also broadly used to identify, then harass or imprison peaceful critics of the regime. In countries ranging from Egypt to Tunisia to Vietnam and China, cybercafes – the cheaper and more popular option for students and less affluent people – are required to monitor users in multiple ways including registration, surveillance cameras, monitoring software installed on computers, and log-in requirements tied to users' national ID numbers or mobile phone numbers making anonymity impossible. Users of cybercafes in many countries have reported that e-mail passwords have been captured and accounts accessed by third parties soon after leaving the café.

    - *"Law enforcement compliance:"* In countries whose governments define "crime" 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 wrong took place when Yahoo's local China-based staff handed over account information of journalist Shi Tao and the activist Wang Xiaoning, and at least two others engaged in political dissent, to the Chinese police.[7] Another example: 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.[8] This happened because Skype delegated law enforcement compliance to its local partner without sufficient attention to how the compliance was being carried out.

    - *Deep packet inspection:* A growing number of nations now have the capability to monitor Internet communications through the use of "deep packet inspection" techniques, or DPI. DPI enables network administrators not only to examine the contents of emails and other communications, but

---

[6] "Internet Enemies," *Reporters Without Borders,* March 12, 2009, at: http://www.rsf.org/IMG/pdf/Internet_enemies_2009_2_-3.pdf

[7] 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

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

also to block and even alter material. In 2008 Global Voices Advocacy Director Sami Ben Gharbia – a Tunisian exile – conducted tests that demonstrated DPI being used in Tunisia to block certain emails, or even alter certain contents of emails like attachments.[9] Deep packet inspection is used in China and Iran. Western companies are assisting in the global spread of this technology. This committee will likely be familiar with a *Wall Street Journal* report last summer which uncovered the fact that a joint venture company between Nokia and Siemens, called Nokia-Siemens Networks, sold deep packet inspection technology to Iran's telecom monopoly as part of a larger sale of mobile-phone networking technology.[10]

- **Cyber-attacks:** The sophisticated, 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.[11] 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 and resources to protect themselves, have over the past few years been victim of increasingly aggressive cyber attacks.[12] The effect in some cases is either to bring down dissident websites at critical political moments or for frequent short periods of time, putting a great strain on the site's operators just to keep the site running and preventing them from doing their main work. Targets range from Chinese human rights defenders to an independent Russian newspaper website, to Burmese dissidents, to Mauritanian opponents of military dictatorship.[13] On December 17, 2009, the home page of Twitter – which was instrumental in spreading world about protests in Iran – was hacked by a group calling itself the "Iranian cyber army." Twitter was back up after a couple of hours. An Iranian green movement website Mowjcamp.com was attacked on the same day but – lacking the same resources

---

[9] "Silencing online speech in Tunisia," by Sami Ben Gharbia, *Global Voices Advocacy,* August 20, 2008, at: http://advocacy.globalvoicesonline.org/2008/08/20/silencing-online-speech-in-tunisia/

[10] "Iran's Web Spying Aided By Western Technology," by Christopher Rhoads and Loretta Chao, *The Wall Street Journal*, June 22, 2009 at: http://online.wsj.com/article/SB124562668777335653.html

[11] *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.

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

[13] "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; "Russia's Novaya Gazeta Web site hacked, paralyzed" by David Nowak, Associated Press, February 1, 2010 at: http://www.washingtonpost.com/wp-dyn/content/article/2010/02/01/AR2010020102424.html ; "Web Sites Back Online, but Fears of Further Attacks Remain," by Min Lwin, *Irawaddy*, September 22, 2008, at: http://www.irrawaddy.org/article.php?art_id=14294 ; "Dictators Prefer Botnets," Strategy Page, November 18, 2008, at: http://www.strategypage.com/htmw/htiw/articles/20081118.aspx

and clout as Twitter – remained offline for more than six weeks.[14] 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. Likewise, journalists who report on human rights problems and academics whose research includes human rights issues 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 activists, these groups are equally unprepared and unequipped to deal with such attacks.[15]

- **Problems of social networks***:* In 2009, Facebook and Twitter served as an important conduit through which Iran's Green Movement has relayed information to the outside world about protests and regime brutality. Iranian exiles living around the world have played a crucial role. Recently, however, the Iranian National Guard has been using Facebook to identify whose exiled relatives have been criticizing the regime from abroad, and then threatening family members living in Iran.[16] Such intimidation tactics are aided by Facebook's cavalier approach to privacy which focuses primarily on the social habits and preferences of American teenagers without adequate consideration of what the same policies might mean for large user communities in places like Egypt, where young people frequently use Facebook to organize protests. To make things even worse, over the past couple of years my colleagues at Global Voices Online have received frequent reports by online activists in a range of countries whose Facebook accounts or groups were shut down at critical times because the American administrators didn't understand the language the activists were using or the political context of their Facebook use, and mistook them for spammers without making any effort to double-check. Such closures can sometimes wreck or seriously debilitate protest-organizing efforts. For example: earlier this month in Hong Kong, a pro-democracy activist who had formed a group to oppose the territory's main pro-China party said his Facebook group containing more than 80 thousand members was shut down suddenly without notice. Other Hong Kong pro-democracy and human rights activists have reported similar shut-downs of Facebook accounts and groups over the past three years, usually during particularly intense times of political activity.[17]

---

[14] "Yahoo!, Moniker: why is Mowjcamp.com still offline 6 weeks after hack attack?" by Ethan Zuckerman, *My Heart's in Accra,* February 1, 2010, at: http://www.ethanzuckerman.com/blog/2010/02/01/yahoo-moniker-why-is-mowjcamp-com-still-offline-6-weeks-after-hack-attack/

[15] "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

[16] "Iranian Crackdown Goes Global," by Farnaz Fassihi, *The Wall Street Journal*, December 3, 2009, at: http://online.wsj.com/article/SB125978649644673331.html

[17] "Facebook questioned as political pages shut down," by Albert Wong and Fanny Fung, *South China Morning Post*, February 6, 2010

Recommendations

Given the wide range of challenges outlined above, it is clear that expanding and protecting global Internet freedom requires a sophisticated, multi-pronged, multi-stakeholder, and truly global approach. While private sector companies have a responsibility to respect and uphold the rights of customers and users, they cannot on their own be expected to solve the political and geopolitical problems that threaten free expression in the first place. Addressing the core problems requires government leadership: from the Administration and from Congress. Thus my recommendations address the private sector as well as the executive and legislative branches.

- **Direct technical support:** The United States government should continue to provide technical support to people whose ability to exercise their right to peaceful expression on the Internet is being quashed or restricted by governments, in some cases with corporate assistance. Congress is to be commended for its allocation of funds over the past few years to support the development of software tools that help Internet users in repressive regimes circumvent Internet filtering. As I have explained, however, regimes are now using a wider range of technical methods to censor Internet content and silence dissent. I would suggest that future funding should support a much broader range of tactics and technologies – along with the training and education in their use – to reflect the growing sophistication with which governments are stifling and silencing peaceful speech. This should include technical assistance, tool development, and training for journalists and members of a broad range of non-governmental organizations in cyber-security as well as anti-surveillance technologies and methodologies.

- **Corporate responsibility:** In order to ensure that American businesses in their activities around the world 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.[18] 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 our air and water or exploit twelve-year-olds, American Internet and telecommunications 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

[18] See http://globalnetworkinitiative.org

governments practice at least one of the forms of Internet controls I've 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. Mr. Chairman as you know, Senator Dick Durbin recently wrote to thirty companies urging them to join the GNI. 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 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.

- *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.

- *Legislation* – Law may be necessary to ensure adequate respect for human rights by companies that do not take voluntary action. 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 U.S. court of law.

  It is important, however, that other laws aimed at promoting corporate social responsibility 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 or categorize. 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 formally categorized as "democratic" or "authoritarian."

- **Upgrade export controls:** Existing export control laws require updating in order to remain consistent with their intent in the Internet age, in two ways:

    - *Halt denial of service human rights activists:* The United States has several laws that bar the sale of specific kinds of software to, or forbid business transactions with, individuals and groups from specified countries. These laws do not take into account new Internet developments, and as a consequence have resulted in denial of website hosting and other services to dissident groups from repressive nations. U.S. laws – exacerbated by corporate lawyers' over-cautious interpretation of them – have recently prevented U.S. web-hosting companies from providing services to opposition groups based in Iran, Syria and Zimbabwe. They should be upgraded as soon as possible so that American Internet businesses can welcome rather than turn away some of the world's most vulnerable and politically isolated groups.[19]

    - *Make collaboration with repression more difficult:* 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 are used for legitimate security and law enforcement as well as repression, it should nonetheless be made more difficult for U.S. companies to provide censorship and surveillance capabilities to governments with a clear track record of using those technologies to suppress peaceful political dissent.

- **Censorship as barrier to trade:** A number of prominent experts in trade law in North America and Europe have argued that Internet censorship should be considered a barrier to trade under the World Trade Organization. In November the European think tank ECIPE concluded that WTO member states are "legally obliged to permit an unrestricted supply of cross-border Internet services."[20] The United States Trade Representative should be encouraged to pursue cases against China and other countries that block their citizens from accessing the online services of U.S. Internet companies.

---

[19] "Not Smart Enough: How America's "Smart" Sanctions Harm the World's Digital Activists," by Mary Joyce, Andreas Jungherr and Daniel Schultz, DigiActive Policy Memo for the Commission on Security and Cooperation in Europe,October 22, 2009, at: http://www.digiactive.org/2009/10/22/digiactive-policy-memo-to-the-us-helsinki-commission/

[20] "Protectionism Online: Internet Censorship and International Trade Law," by Brian Hindley and Hosuk Lee-Makiyama, ECIPE Working Paper No. 12/2009, at: http://www.ecipe.org/protectionism-online-internet-censorship-and-international-trade-law/PDF

- **Universal accountability and rule of law:** In order to uphold and protect the rights of users and customers around the world, American companies must strive for maximum accountability and rule of law in their relationships with governments. Their ability to do so will be reduced - and their efforts easily discredited by foreign governments - if their relationships with U.S. government agencies are not conducted according to the highest possible standards of rule of law and public accountability. The Electronic Privacy Information Center (EPIC) – on whose advisory board I currently sit – has submitted written testimony requesting that this Committee ask Google to publicly disclose the nature of its relationship with the National Security Agency, and to support disclosure by the NSA of the text of National Security Presidential Directive 54, which sets forth the agency's role in cybersecurity and surveillance.[21] In acting to protect the American people's rights from violation as a result of potentially unlawful actions carried out by companies at the behest of U.S. government agencies, and by insisting upon maximum public oversight and respect for rule of law in law-enforcement and national defense-related interactions between American companies and government agencies, this Committee can send two important messages to the world. First, we as Americans do in fact practice what we preach. Second, U.S. companies are not nebulous extensions of the United States government, as their competitors in some markets like to claim. Congress can do much to strengthen American ICT companies' credibility and competitiveness around the world by insisting on one set of global, universal standards of accountability and rule of law in all public-private relationships.

- **Support the Council of Europe Privacy Convention:** Written testimony submitted to this Committee by the Electronic Privacy Information Center (EPIC) also urges this Committee to support the Council of Europe Convention on Privacy, which "aims to ensure that the rights of the individual would be protected even as governments and private organizations took advantage of new systems of automation."[22] Mr. Chairman, support by this Committee for the Council of Europe Convention on Privacy would send a clear message to the world that we as Americans aim to hold our companies to the same high standards of privacy and civil liberties protections at home and in other democracies, as when they are operating in authoritarian nations.

- **Continued executive leadership.** Secretary of State Clinton's landmark speech on Internet freedom made it clear that this is a core American value and priority. She has placed the United States squarely in a leadership position by identifying a range of threats to Internet freedom as well as the range of tools and policies that can be brought to bear. In reviving the Global Internet Freedom Task Force

---

[21] "Statement for the Record of The Electronic Privacy Information Center (EPIC)," by Marc Rotenberg, Matthew Phillips, and Jared Kaprove. Hearing on "The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade" before the Committee on Foreign Affairs, U.S. House of Representatives February 10, 2010. http://epic.org/privacy/cloudcomputing/google/EPIC_Cybersecurity_Statement.pdf

[22] Ibid.

(GIFT), the Administration now has a mechanism to coordinate between government, industry, and civil society to ensure that U.S. companies play a constructive role around the world. GIFT will also need to tackle the even more challenging job of coordinating between all the different U.S. government agencies whose work touches upon the Internet in various ways. If we are serious about promoting global Internet freedom, it is important that U.S. foreign policy, trade, commerce, and national security all be consistent in supporting this goal.

As Secretary Clinton pointed out, more connectivity is not an unfettered good. The Internet is also used to commit all kinds of crimes, exploit children, recruit terrorists, and launch cyber-attacks. These problems call for smart and innovative diplomacy. She called for new tools to help law enforcement agencies cooperate across jurisdictions, and for coordination to prevent debilitating cyber-warfare. As she pointed out, in coordinating domestic and international law enforcement and anti-terror efforts, we need to avoid legal and technical solutions that would make it more difficult or even impossible for dissidents and whistleblowers around the world to speak truth to power.

Therefore, Mr. Chairman, I respectfully appeal to your Committee to consider the following: In negotiating trade agreements on intellectual property, the United States must lead the world in finding solutions that will support our creative industries, but which also will not involve strengthening intermediary liability in ways that will require companies to censor and monitor users. We must resist the temptation to allow widespread commercial use of deep packet inspection technologies – which make it easy to track piracy and crime, but which can so easily be abused by powerful incumbents as well as dictators.

Conclusion:

One of the great challenges of our generation is to find the right balance in the Internet age between society's need for security on the one hand, and the imperative of human rights and civil liberties on the other. The United States is in a position to seek innovative solutions and lead a global dialogue about the new challenges posed by the Internet to *all* governments, most companies, and most parents for that matter. The U.S. can play a leading role in bringing together governments, companies and concerned citizens to find solutions to difficult new economic and security problems. We must take the lead in ensuring that security solutions, economic strategies, and business deals - at home and abroad - will truly enhance the development of a free and open global Internet.