Testimony of

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

At the hearing:
"Global Internet Freedom and the Rule of Law, Part II"

Senate Judiciary Committee
Subcommittee on Human Rights and the Law

March 2, 2010

Thank you, Mr. Chairman, for the opportunity to testify today. I am a great admirer of your tireless leadership on issues related to Internet freedom, civil liberties, human rights, and corporate social responsibility. I look forward to answering your questions, along with those of Ranking Member Senator Coburn, and other esteemed members of this Subcommittee.

My name is Rebecca MacKinnon. I am currently a visiting fellow at Princeton University's Center for Technology Policy. Earlier in my career I worked as a journalist for CNN in China, living in Beijing for more than nine years. For the past 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, the 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 and reported on authoritarian controls firsthand; 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.

After describing how authoritarianism is adapting to the Internet - in ways that involve companies - I will offer some specific policy recommendations, addressed to companies as well as to the U.S. government.

Authoritarianism is adapting to the Internet

Technology 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. I myself have heard such arguments made here on Capitol Hill numerous times, beginning with the February 2006 hearing on Internet freedom chaired by the late Representative Tom Lantos. As time passes, however, people like myself who study the Internet and global politics are finding that the reality isn't so simple - and the future isn't automatically rosy just because the Internet exists and connectivity is spreading. Internet and mobile phones *have* empowered many people around the world, and they *do* have the potential to facilitate greater freedom and democracy. But more connectivity doesn't automatically lead to more freedom. Other political, legal, and technical factors affect whether it's possible for communication technology to live up to its potential.

In the four years since the late Rep. Lantos' famous February 2006 hearing where Google, Yahoo, Microsoft and Cisco first defended their business practices in China, the number of Internet users on the planet has almost doubled. Yet according to the latest "Freedom of the World" study released by Freedom House, the overall level of freedom in the world declined in 2009 for the fourth consecutive year.[1] Ironically, many of the countries with the most serious declines in freedom are also experiencing rapid growth in Internet and mobile usage. Take China, for example. The number of Chinese Internet users quadrupled in the past four years. It is true that the Internet has enabled people to expose corruption, bring justice to innocent victims of official malfeasance, and even change some laws and regulations, in ways that were not possible in the past. But this has not led to the overall strengthening of rule of law, greater independence of the courts from the Communist Party, or greater protection of civil liberties by the system as a whole. According to 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, and the trend is expected to continue when figures come out for 2009.[2] China is pioneering new, flexible but effective methods 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 reform movements from succeeding, or in some cases even from emerging.

China is now the model for authoritarian survival in the Internet age. The Chinese Communist Party fully recognizes that it is no longer possible for a nation to be economically competitive without being connected to the global Internet. Rather than try to restrict connectivity, modern authoritarian governments are working aggressively to

---

[1] *Freedom in the World 2010,* by Freedom House, February 2010, at: http://www.freedomhouse.org/template.cfm?page=505

[2] "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

use Internet and mobile technologies to their own advantage. Iran is one of China's most eager students, as the Ahmadinejad regime finds ways to counter the Green Movement's use of technology. 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.[3] Last month Iran's chief of police warned protestors against using e-mail, text messaging and social networks to organize demonstrations. "The new technologies," he said, "allow us to identify conspirators and those who are violating the law without having to control all people individually."[4]

The inconvenient truth is that authoritarianism is adapting to the Internet age. Google's recent public challenge to the Chinese government's cyber-attacks and censorship took place in this broader context. In my view it shows a recognition that the *status quo* – in terms of authoritarian censorship, regulation, and manipulation of the Internet – will not necessarily improve any time soon, and could continue get worse unless a broader range of companies, citizens, and governments, realize what's happening and take responsibility for the future of freedom in the Internet age.

The expanding toolbox of Internet controls

Governments seeking to control online speech began their efforts in the late 1990s with "filtering" or "blocking" of web content. Today, modern authoritarian regimes have at their disposal an expanding toolbox of technical, legal, commercial and political mechanisms to censor, manipulate, and monitor citizens' online speech. In addition to the classic filtering and blocking with which this Subcommittee is most familiar, other techniques used by regimes to restrict Internet freedom that involve technology companies include: deletion of content, device and local-level controls, surveillance, and cyber-attacks. For the record, I will explain each of these briefly:

- **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 – including SmartFilter now sold by McAfee – are

[3] "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

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

developed and marketed here in the United States by U.S. companies for use 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. As this Committee is well aware, 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.[5]

- **Deletion and takedown of content by Internet companies:** 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.[6] 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

[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] 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

Chinese bloggers. Politically sensitive conversations are deleted or blocked from being published at all. 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.[7]

- **Cyber-attacks:** The sophisticated, military-grade cyber-attacks launched against Google were targeted specifically at the 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 and resources to protect themselves, have over the past few years been victim of increasingly aggressive cyber attacks.[8] 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.[9] 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 and clout as Twitter and hampered by U.S. laws that forbid American web hosting companies from doing business directly with Iranians – remained offline for more than six weeks.[10]

  In other cases cyber attacks 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.

---

[7] 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

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

[9] "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

[10] "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/

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.[11]

- **Compliance with political "law enforcement":** 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. This committee is of course very familiar with the most notorious example of law enforcement compliance gone wrong: between 2002 and 2004 Yahoo's local China-based staff handed over to the Chinese police e-mail account information of journalist Shi Tao, activist Wang Xiaoning, and at least two others engaged in political dissent.[12] There are other examples. 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.[13] This happened because Skype delegated law enforcement compliance to its local Chinese partner without sufficient attention to how the compliance was being carried out.

- **Device-level and local controls:** In late spring of 2009 the Chinese 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."[14] 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.[15] The

---

[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] 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

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

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

[15] *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/.

software had other problems that 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.[16] The defeat of Green Dam, however, did not diminish other efforts to control and track Internet users at more localized levels inside 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.[17] The implementation of these systems has received little attention outside of China.

Recommendations

Given the mounting challenges outlined above, it is clear that a policy aimed at supporting 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 companies and civil society as well as the executive and legislative branches.

- **Corporate responsibility:** In order to ensure that American businesses 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.

  Mr. Chairman, your recent letters to thirty companies in the Information, Communications and Technology (ICT) sector were an important step in advancing an urgent conversation about how we can help American companies compete and succeed in the global marketplace while at the same time upholding core values of privacy and freedom of expression. Only a few months after your last hearing on this subject in May 2008, Google, Yahoo, and Microsoft took the

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

[17] "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/

important step of joining the Global Network Initiative (GNI), a code of conduct for free expression and privacy in the ICT sector. 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, 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 can benefit from Internet and mobile technologies. In most cases companies can contribute to economic prosperity and individual empowerment by being engaged in countries whose governments practice some of the 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 fundamentally reasonable to expect all companies in the ICT sector 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 most from these technologies. All GNI members are participating in this process because we believe in the transformative importance of the ICT sector and want innovative businesses to be successful and competitive. We are working with companies in good faith. I personally believe that the GNI member companies are managed by people who want both to do well and to do good, but who recognize that they face difficult problems, and that they could use support and advice in order to avoid mistakes. As an academic researcher and free speech advocate, my goal in working with GNI member companies is to help them foresee and avoid mistakes long before they happen. When mistakes do happen, companies should be held appropriately accountable in ways that can help the entire industry learn from these mistakes and do a better job of avoiding them in the future.

GNI's principles are supported by implementation guidelines and an accountability framework that 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. 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 clear that the thirty companies contacted by you, Mr. Chairman, 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.

- **Legislative measures:** Congress has a range of legislative tools at its disposal. Some should be implemented as soon as possible, while others may take more time and consideration in order to ensure that they are proportional, appropriate, and effective.

    - ***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 U.S. court of law.

    - ***Incentives for socially responsible innovation:*** Established companies as well as entrepreneurial new startups should be encouraged, perhaps through tax breaks and other incentives, to develop technologies and features that enhance users' ability to evade censorship and surveillance, as well as to help users better understand what personal information is being stored, how it is used, and who has access to it.

    - ***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 to 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.[18]

        - 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

[18] "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/

governments with a clear track record of using those technologies to suppress peaceful political dissent.

- ***Technical support for free expression:*** People in repressive regimes require support in a broad range 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. In addition to helping people around the world to circumvent Internet blocking, we need to help people fight cyber-attacks, counter-act content removal by companies, fight deployment of device-level spyware and censorware, and educate each other quickly about new forms of technical control as new methods and technologies emerge.

    - Circumvention technologies: Congress deserves great praise for its allocation of funds over the past few years to support the development of tools and technologies that help Internet users in repressive regimes circumvent Internet filtering. Support for a healthy range of circumvention tools – in a manner that fosters competition, innovation, accountability, and user choice – is important and must continue. The problem is that circumvention tools only address Internet filtering: they don't address other methods of control that repressive regimes now use to censor Internet content and silence dissent. Thus, an effective Internet freedom strategy cannot focus on circumvention alone.

    - Anonymity and security: In my interactions with journalists, human rights activists, civil liberties lawyers, bloggers, and academics in authoritarian countries around the world, I have found that a shockingly large number are uninformed 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. Local-language, culturally appropriate technologies, accompanied by robust education and training, is desperately needed. The recent cyber-attacks against Chinese GMail users only highlights the urgency.

    - Preservation and re-distribution of deleted content: In the course of my research about the Chinese Internet, I have noticed that quite a lot of people around Chinese blogosphere and in chatrooms make a regular habit of immediately downloading interesting articles, pictures, and videos which they think those materials could get deleted or taken offline. They then re-post these materials in a variety of places, and relay them to friends through social networks and e-mail lists. This is done in an ad-hoc way. Thus, it is often difficult for people to locate and spread this material. The United States should support the creation of searchable, accessible, and

secure repositories of censored materials from countries where companies are systematically required to delete and take down politically sensitive material. Combined with robust circumvention tools, such repositories could do much to counter-act the effects of widespread content deletion and takedown within authoritarian countries.

- Distributed "opposition research": After the Chinese government mandated the nation-wide installation of the "Green Dam" censorware last year, loosely organized "opposition research" networks sprang into action. 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.[19] This information was then used by domestic and foreign opponents of Green Dam in a successful campaign to reverse the government's mandate. Another anonymous group of Chinese netizens have collected a list of companies and organizations – domestic and foreign – who have helped build China's Internet censorship system.[20] Opposition research has also helped to expose the Tunisian government's use of cutting-edge "deep packet inspection" techniques for censorship and surveillance. 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.[21] If people in repressive regimes had better mechanisms through which to collect and share information about how their governments are stifling free expression, it would be easier for activists around the world to help each other develop effective technologies and tactics to fight back.

- ***Other legislative measures:*** Further legal steps may be necessary to ensure adequate respect for human rights by companies that fail to take voluntary action. It is important, however, that any law be flexible enough to accommodate the rapidly-changing nature of information communications technology, as well as the complex and highly diverse

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

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

[21] "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/

nature of ICT businesses – including many small startups, as well as innovations that are difficult to define or categorize. It is important that any law concerning the human rights implications of ICTs be truly global in scope, recognizing that companies face human rights dilemmas in almost every market. Furthermore, the extent to which any given country might be considered "free" or "repressive" can change overnight with a coup or rigged election.

- **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."[22] 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.

- **Continued executive branch leadership.** Secretary of State Clinton's landmark speech on Internet freedom made it clear that this is a core American value. 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 (GIFT), the Administration now has a mechanism to coordinate between government and industry to ensure that U.S. companies play a constructive role around the world. GIFT will also need to tackle the 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 advancing Internet freedom.

Conclusion

There is no "silver bullet" for global, long-term and sustainable Internet freedom. Offline physical freedom here in the United States - or anywhere else for that matter - was not won easily, and cannot be expanded, preserved or protected without constant struggle and vigilance. Internet freedom is no different. A global struggle for freedom and control of cyberspace is now underway. As with our physical freedom, Internet freedom will not be possible without a supportive ecosystem of industry, governments, and concerned citizens working together. Chairman Durbin, Ranking Member Coburn, and all other members of this Subcommittee, I commend you for taking historic first steps in building the global support system for Internet freedom.

---

[22] "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