# THE GOOGLE PREDICAMENT: TRANSFORMING U.S. CYBERSPACE POLICY TO ADVANCE DEMOCRACY, SECURITY, AND TRADE

## HEARING

BEFORE THE

## COMMITTEE ON FOREIGN AFFAIRS
## HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

MARCH 10, 2010

**Serial No. 111–85**

Printed for the use of the Committee on Foreign Affairs

Available via the World Wide Web: http://www.foreignaffairs.house.gov/

U.S. GOVERNMENT PRINTING OFFICE

55–395PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

## COMMITTEE ON FOREIGN AFFAIRS

HOWARD L. BERMAN, California, *Chairman*

GARY L. ACKERMAN, New York
ENI F.H. FALEOMAVAEGA, American Samoa
DONALD M. PAYNE, New Jersey
BRAD SHERMAN, California
ELIOT L. ENGEL, New York
BILL DELAHUNT, Massachusetts
GREGORY W. MEEKS, New York
DIANE E. WATSON, California
RUSS CARNAHAN, Missouri
ALBIO SIRES, New Jersey
GERALD E. CONNOLLY, Virginia
MICHAEL E. MCMAHON, New York
JOHN S. TANNER, Tennessee
GENE GREEN, Texas
LYNN WOOLSEY, California
SHEILA JACKSON LEE, Texas
BARBARA LEE, California
SHELLEY BERKLEY, Nevada
JOSEPH CROWLEY, New York
MIKE ROSS, Arkansas
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
JIM COSTA, California
KEITH ELLISON, Minnesota
GABRIELLE GIFFORDS, Arizona
RON KLEIN, Florida
VACANT

ILEANA ROS-LEHTINEN, Florida
CHRISTOPHER H. SMITH, New Jersey
DAN BURTON, Indiana
ELTON GALLEGLY, California
DANA ROHRABACHER, California
DONALD A. MANZULLO, Illinois
EDWARD R. ROYCE, California
RON PAUL, Texas
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
JOE WILSON, South Carolina
JOHN BOOZMAN, Arkansas
J. GRESHAM BARRETT, South Carolina
CONNIE MACK, Florida
JEFF FORTENBERRY, Nebraska
MICHAEL T. MCCAUL, Texas
TED POE, Texas
BOB INGLIS, South Carolina
GUS BILIRAKIS, Florida

RICHARD J. KESSLER, *Staff Director*
YLEEM POBLETE, *Republican Staff Director*
SHANNA WINTERS, *General Counsel and Senior Policy Advisor*
GENELL BROWN, *Senior Staff Associate/Hearing Coordinator*

# CONTENTS

Page

WITNESSES

Nicole Wong, Esq., Vice President and Deputy General Counsel, Google, Inc. .. 9
Ms. Rebecca MacKinnon, Visiting Fellow, Center for Information Technology Policy, Princeton University, Cofounder of Global Voices Online ..... 19
Larry M. Wortzel, Ph.D., Commissioner, U.S.-China Economic and Security Review Commission ..... 32
Mr. Robert W. Holleyman, II, President and CEO, Business Software Alliance ..... 45

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Nicole Wong, Esq.: Prepared statement ..... 12
Ms. Rebecca MacKinnon: Prepared statement ..... 21
Larry M. Wortzel, Ph.D.: Prepared statement ..... 34
Mr. Robert W. Holleyman, II: Prepared statement ..... 48
The Honorable Christopher H. Smith, a Representative in Congress from the State of New Jersey: Letter from Google, NGO Joint Statement in Support of H.R. 2271 and letter from Freedom House ..... 81

APPENDIX

Hearing notice ..... 92
Hearing minutes ..... 93
The Honorable Howard L. Berman, a Representative in Congress from the State of California, and Chairman, Committee on Foreign Affairs: Prepared statement ..... 95
The Honorable Eni F.H. Faleomavaega, a Representative in Congress from American Samoa, and Chairman, Subcommittee on Asia, the Pacific and the Global Environment: Prepared statement ..... 97
The Honorable Russ Carnahan, a Representative in Congress from the State of Missouri: Prepared statement ..... 100
The Honorable Gerald E. Connolly, a Representative in Congress from the State of Virginia: Prepared statement ..... 101
The Honorable Gene Green, a Representative in Congress from the State of Texas: Prepared statement ..... 102
Questions submitted for the record by the Honorable Barbara Lee, a Representative in Congress from the State of California ..... 103
Question submitted for the record by the Honorable Ileana Ros-Lehtinen, a Representative in Congress from the State of Florida ..... 114
Questions submitted for the record by the Honorable Joseph Crowley, a Representative in Congress from the State of New York ..... 115
Question submitted for the record by the Honorable Christopher H. Smith, a Representative in Congress from the State of New Jersey ..... 116
Questions submitted for the record by the Honorable Michael T. McCaul, a Representative in Congress from the State of Texas ..... 117

# THE GOOGLE PREDICAMENT: TRANSFORMING U.S. CYBERSPACE POLICY TO ADVANCE DEMOCRACY, SECURITY, AND TRADE

---

**WEDNESDAY, MARCH 10, 2010**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON FOREIGN AFFAIRS,
*Washington, DC.*

The committee met, pursuant to notice, at 10:04 a.m. in room 2172, Rayburn House Office Building, Hon. Howard L. Berman (chairman of the committee) presiding.

Chairman BERMAN. The committee will come to order. Just for the three colleagues of mine who are here now, I would like to remind you that at 8:30 a.m. tomorrow I will be hosting a meeting of the Foreign Assistance Reform Working Group in room 2255, and I encourage my colleagues to come. Next week at 9:30 a.m. we will have what promises to be a very interesting hearing on the European security architecture and the transatlantic security architecture.

And sometime before the spring recess I hope to hold a markup to consider Mr. Smith's International Megan's Law legislation and possibly a bill on science diplomacy which Mr. Fortenberry and I will introduce today.

After Mr. Smith and I make our opening remarks, other members will have the opportunity to make 1-minute statements if they wish to do so. Members are also welcome to place written statements in the record. In fact, for the members who are here now, I think—and given that the Afghanistan legislation is not going to be on until later—for the members who are here at the time of the gavel, I think we will allow 2-minute opening statements by them.

Today's hearing: In a recent speech on 21st-century statecraft, Secretary Clinton said the State Department is realigning its policies and priorities to harness and promote the power of the latest communication tools. Her remarks illustrate the fact that new means of electronic communication have created both opportunities and challenges for those who formulate our national security and foreign policy.

While many congressional committees have looked at the issues of human rights, defense, and trade in connection with the Internet, it is time for us to consider a comprehensive approach to the increased worldwide use of cyber technology.

This hearing will address what we are calling the "Google Predicament" because Google's experience over the past couple of months highlights the challenges in developing a cyber-specific foreign pol-

icy. The Internet is a useful tool to promote freedom and trade, but in some places it also serves as a means of censorship. It is a boon for U.S. business but also a source of great vulnerability with respect to U.S. national security. Reconciling these conflicting policy challenges is a key mission for the administration and, I believe, for this committee.

The latest communication technologies are being put to use to advance democracy and protect human rights. Widespread use of Twitter overcame the Iranian regime's ban on media coverage of last summer's election results and their aftermath. And a graphic video posted on YouTube of a young Iranian woman who was shot and killed during a protest galvanized world opinion, as it gave people an unvarnished look at the crackdown.

The administration acknowledged the power of these communication tools just this past Monday by granting a general license for the transfer of social networking software to Iran and other repressive nations. This is an important and good step that will foster greater freedom of expression. But paradoxically, cyber technology also serves as a weapon of choice for repressive regimes. Under our former chairman, Tom Lantos, this committee examined closely how American companies, however passively, can and do facilitate censorship. Our colleague Chris Smith has also been very active in advancing the discussion of this subject.

The notion that American companies can heedlessly supply their software, routers, and information to governments that use them for repressive purposes is untenable. But preventing companies from engaging in trade with countries ruled by those repressive governments is equally untenable, for it would deny billions of people the ability to access the very information needed to support their resistance.

When it comes to human rights, there must be a way to balance the benefits of cyber technology with its very real potential harms. A voluntary organization known as the Global Network Initiative, made up of human rights organizations and various companies, works directly on this issue. Regrettably, many companies have failed to join. As a result, we may consider legislation to address this issue. Providers of technology need to step up.

American companies did just that last year when Beijing mandated installation of the Green Dam-Youth Escort Software on all computers sold in China. This software program would have blocked Internet searches on politically sensitive subjects and made computers more vulnerable to hackers. Companies persuaded the United States Government to protest the Green Dam requirement because it violated free trade obligations under WTO rules. We need to see that kind of public-private partnership at work across the board on issues involving cyber security and Internet freedom.

It is also very much in the interest of U.S. business to make such a partnership work. Brand integrity of U.S. entities is at stake when someone hacks into and alters or steals the intellectual property of U.S. companies such as Google. Melissa Hathaway, author of President Obama's recent "Cyberspace Policy Review," suggests that the government may need to retool our intelligence and diplomatic communities to protect U.S. intellectual property abroad.

Finally, and perhaps most troubling, is the way cyber technology can be exploited to undermine our own security. Make no mistake: Not only are sophisticated and network-secure companies like Google vulnerable to attack from foreign countries, but the entire U.S. network faces assault on a daily basis. As recently noted by Deputy Defense Secretary Lynn, an adversarial nation could deploy hackers to take down U.S. financial systems, communications and infrastructure at a cost far below that of building a trillion-dollar fleet of jet fighters or an aircraft carrier.

China's alleged hacking of Google and subsequent reports that Google is partnering with the National Security Agency to analyze the attack raise some relevant questions for this committee: Does an unauthorized electronic intrusion constitute a violation of national sovereignty, equivalent to a physical trespass onto U.S. territory—and if so, what is the appropriate response?

We also need to consider the foreign policy implications of offensive U.S. capabilities. The United States has much to lose from a lawless cyberspace where countries can attack each other at will and engage in a perennial low-intensity cyber conflict.

We look forward to hearing from our witnesses on how we can simultaneously promote Internet freedom and deprive repressive regimes of the tools of cyber-repression; and how we can promote the global diffusion of the Internet while also protecting ourselves from cyber attack.

But before we hear from our witnesses, first let me turn to our esteemed colleague, Chris Smith—designated by the ranking member to serve in her stead today—for any opening remarks that he may wish to make.

Mr. SMITH. Mr. Chairman, thank you very much, and I thank you for convening this very timely and very important hearing. Mr. Chairman, as you know, Reporters Without Borders documents that at least 120 people are currently imprisoned for online postings, that is the ones we know of, 72 of them in China alone, but also large numbers in Iran and Vietnam. In 2005, I had a meeting in a restaurant in Hanoi with Vu Thuy Ha, the wife of Dr. Pham Hong Son, who had e-mailed an article entitled "What is Democracy?," downloaded from U.S. Embassy in Hanoi's Web site.

He sent it to his friends. The Vietnamese Internet police called this espionage and punished him with a very long prison term. While Vu and I talked, police thugs conspicuously sat at the next table—there were three of them—scowled at her, took her picture, I took theirs, and they made a number of threatening gestures. She was very fearful. Many people in this room will remember the groundbreaking hearings this committee held on Internet freedom.

I chaired two of those in 2006, I chaired an 8-hour hearing on the Internet in China, which we subtitled "A Tool for Freedom or Suppression." The hearing responded to Yahoo's cooperation with Chinese Internet police in tracking down journalist Shi Tao, who is still serving a 10-year prison term for disclosing state secrets—that is, he e-mailed to the United States Chinese Government orders on not reporting on the 15th anniversary of the Tiananmen Square massacre—he sent that to an NGO in New York.

In 2007, Tom Lantos followed up with a hearing on Shi Tao and others in which Yahoo's Jerry Yang testified to the committee

while Shi Tao's mother sat right behind him in the audience. At the end of the hearing, Jerry Yang met with Shi Tao's mother, and since then Yahoo has undertaken to do what it can to compensate some of the families like Shi Tao's and others imprisoned because of their Internet work. But the victims of the growing global assault on Internet freedom are also entire peoples denied their right to free expression, often self-censoring out of fear, and denied access to information.

These include the Chinese, Iranian, Belarusian, Cuban, Burmese, Egyptian, North Korean, Saudi Arabians, Syrian, Tunisian, Turkmen, and Uzbek peoples, who live under governments which Reporters Without Borders classifies as the twelve worst enemies of the Internet. Currently, over three dozen countries routinely censor the Internet. This number is growing. And in recent years they have developed increasingly sophisticated tools for blocking, filtering, and surveilling the Internet. They exchange technologies and tactics, which are often modeled on the Chinese Government's Great Firewall of China.

Yet we have also learned some positive lessons from 2006. We have seen that many U.S. IT companies really want to do the right thing. Since 2006, Yahoo has established much stricter policies governing its interactions with repressive governments, working to keep personally identifying information out of their hands. When it went into Vietnam, for example, Yahoo stored personally identifiable information in Singapore, out of reach of the government secret police.

Google's transformation has even been more remarkable. Since 2006, I have been meeting with Google executives and they have known for some time that the theory that their mere presence in the Chinese market would somehow liberalize China or at least justify their willingness to censor searches has proven mistaken, and that China was growing more repressive. Google's statement in January that it "is no longer willing to continue censoring results on its Chinese search engine" was remarkable and it was thrilling. Certainly the hearts of millions of Chinese human rights activists and political dissidents were equally happy.

Google deserves to be praised for this decision. It is a blow against the cynical silence of so many about the Chinese Government's human rights abuses, a blast of honesty and courage from which we can all draw inspiration. Mr. Chairman, I believe Google's making a principled and public commitment to do the right thing and stop censoring, combined with its willingness to spend some time in patient dialogue with the Chinese Government, giving that government every chance to do the right thing as well, is a model of how IT companies can deal with repressive regimes.

But I also believe the model can be improved upon. Google's recent difficulties in China make it even more clear, clearer than ever, that however well intentioned American IT companies are, they are not powerful enough to stand up to a repressive government, particularly the likes of China. Without U.S. Government support and backing, they are inevitably forced to play a role in the repressive government censorship and surveillance.

But the Global Online Freedom Act, legislation I crafted in '06 and reintroduced this Congress, will give American IT companies

the U.S. Government backup they need to negotiate with repressive governments. I would remind my colleagues it was patterned after three major initiatives, the International Religious Freedom Act of 1998, the Trafficking Victims Protection Act of 2000, which I authored, and the Foreign Corrupt Practices Act, which in the late '70s, many people said that it disadvantaged U.S. companies. Yet, it really became the model—not just for the U.S. but for the world—on not providing bribes and other such ways of doing business all over the world.

It is the standard, it is a model, and is a minimum standard that needs to be followed now on the Internet side. Because of time, I will not go through all of the various provisions of the Global Online Freedom Act, but I would ask my colleagues to take a good hard look at it. I think it is an idea whose time has come in terms of really setting at least a minimal standard, a floor if you will, to protect nonviolent political speech and nonviolent religious speech; and that is the aim of the legislation.

It does it in two very simple ways: By requiring a full disclosure of what it is that is being censored, and secondly, by ensuring that personally identifiable information is put out of reach of Internet restricting countries, a designation that would be conferred on those countries after due diligence and analysis by an office that would be created within the Department of State. I thank you, Mr. Chairman, for again calling this hearing. We need to move on this and move quickly. Thank you.

Chairman BERMAN. Time of the gentleman has expired. Under the unanimous consent edict or whatever, the members who were here at the time, if they wish to, can be recognized for up to 2 minutes. Other members who wish to make opening statements for 1 minute. The gentleman from California, Mr. Sherman, seeks recognition? The gentleman is recognized for 2 minutes.

Mr. SHERMAN. American policy is marked by perhaps a very aggressive military policy and a very passive approach to using our economic, technological, and diplomatic power. Keeping Google out of China is not the solution, in fact that may be what China is trying to achieve. We should instead have hundreds of millions of dollars devoted to developing the technology and putting out the contracts to develop the technology to punch a hole in the Great Wall of China and all the other barriers to the use of the Internet.

Likewise, we should be aggressive in using our technology to take down terrorist sites around the world. But this isn't just an Internet issue, this is an overall economic issue. We have an enormous trade deficit with China because we open our markets to them and they figure out ways to close their market to us. Hacking is just one of many ways they do that. We have had hearings in our Subcommittee on Terrorism, Nonproliferation and Trade, in which business after business comes forward and talk about what they face when they try to export to China. The offsets, the criminality, the theft, the confiscation and our Government does nothing. As long as American policy is dominated by Wall Street and Wal-Mart, neither democracy nor America will be in the ascendancy. I yield back.

Chairman BERMAN. The gentleman has yielded back. Does the gentleman from California seek recognition?

Mr. ROHRABACHER. Yes I do.

Chairman BERMAN. The gentleman from California, Mr. Rohrabacher, is recognized for 2 minutes.

Mr. ROHRABACHER. Thank you very much. And I would like to identify myself with the remarks of my colleague, Mr. Sherman, who is again getting to the heart of the matter in many ways. Let us just note, in January of this year when Google announced its intention to stop censoring its search results in the People's Republic of China, I was very supportive and I was very complimentary of Google, and because that was in stark contrast to some of the other companies that were operating in China.

Unfortunately, Google has yet to follow through on and to stop self-censoring. And, you know, our praise shouldn't be for an intent, our praise should be for accomplishing what has been set out, and I am very anxious today, Mr. Chairman, to hear the details about what Google is planning to do, and there seems to be a contradictory position here between what their goal is and what they are actually doing as we speak. Let us note that the Internet is a powerful force in the world today, and I would suggest it can be used for positive things, it can be used to promote freedom and human dignity and information, the spread of information over a broad area, or it can be used for just the opposite, it could be used by tyrants and gangsters to oppress their own people.

It behooves us, as people who believe in freedom and democracy, to stand with the people of China and to say that in this very important area of technology transforming our societies, that we will work with the people of China, not the Government of China, to see that this technology is used in a positive way and not a negative way. If, as Mr. Sherman says, if our corporations hold true to those values, we will work with those corporations. If the corporations that happen to be owned by Americans do not, we will be against them.

Chairman BERMAN. The time of the gentleman has expired. Who else seeks recognition for opening statements? The gentlelady from California, Ms. Woolsey, is recognized for 2 minutes.

Ms. WOOLSEY. Thank you, Mr. Chairman. I will be very quick. China is a very desirable market, and that makes it that much more difficult for us and the corporations in China to take a principled stand against, well, our corporations to take a principled stand against China's cyber action and policies. That is very clear to us. But of course we must take a stand. And it would certainly be best, as Congressman Rohrabacher said, if the corporations and businesses in China and the United States would work out our differences and make this work. But if it can't, I support our chairman in saying that we will need to take action. So I am so anxious to hear today what our witnesses have to say because I bet you have some good ideas about this. And I would like to yield the rest of my time to Congresswoman Lee from California.

Chairman BERMAN. The gentlelady yields 1 minute to the gentlelady from California, Ms. Lee.

Ms. LEE. Thank you, Mr. Chairman. Let me thank the gentlelady for yielding and just welcome our panelists and just say, you know, while these very powerful technologies have provided many opportunities to improve lives as well as strengthen international en-

gagement and partnership, they have also opened doors for misuse or abuse by governments, businesses, and individuals. Adapting and planning for the current and anticipated impact of this technological transformation is really critical for us to ensure that we take a very proactive approach to fostering the flow of information, guarding our vital national security interests, and protecting individual freedoms and civil liberties for ours and for future generations. Thank you again, Mr. Chairman. I want to thank again the gentlelady for yielding, and welcome, look forward to your testimony.

Chairman BERMAN. Time of the gentlelady has expired. Anyone else seek recognition for an opening statement? The gentleman from South Carolina, Mr. Inglis, is recognized for 1 minute.

Mr. INGLIS. Thank you, Mr. Chairman. When I was practicing law in about 1999, the assistant IT person at our firm handed me a piece of paper, he said, "Google"—he had written it out—he said, "Google, that is what you want to go search on." Now, like I suppose most people, I am frustrated by any other search engine, because they are not as fast and they are not as good as Google. So the thought of having a real Google and a fake Google, one that turns up all the results that the rest of the world can see, and one that turns up just what the Chinese Communist dictators want you to see, is just an amazing incongruity, it just doesn't make sense. And so I am so grateful for Google recognizing that and making the decision to move toward providing the people of China with the real Google, the real information that the rest of the world gets. That is the way it should be. Thank you, Mr. Chairman.

Chairman BERMAN. The time of the gentleman has expired. The gentleman from New York, Mr. Crowley, seeks recognition. The gentleman is recognized for 1 minute.

Mr. CROWLEY. Mr. Chairman, thank you very much. I also want to thank Ranking Member Ros-Lehtinen for organizing this hearing. I would also like to thank the witnesses for their willingness to share their experiences. It is no secret that there are different opinions on doing business in China, especially when it comes to matters relating to freedom of expression. At the same time, we know that those with differing views are acting in the spirit as Confucius's famous saying goes, hold faithfulness and sincerity as first principles. These issues, the security of the Internet, intellectual property, and indeed national security, go to the very core of our national interests. I look forward to hearing more from the witnesses on these important matters and this timely discussion. With that, Mr. Chairman, I yield back 20 seconds.

Chairman BERMAN. Yes, that and what gets you a cup of coffee? The gentleman from California, Mr. Royce, is recognized for 1 minute.

Mr. ROYCE. Thank you, Mr. Chairman. Information is power, and during the Cold War, radio free Europe in its broadcasts helped to spread untainted information that empowered people like Lech Walessa and Vaclav Havel. But today the means have changed, but the ability of information to undermine totalitarian regimes remains constant. The Internet has empowered new generations. You have the green movement in Iran that has utilized new technologies to disseminate information among dissidents, democracy

advocates from China to Vietnam are blogging about freedom and about democracy. But I will close with this irony, and it is from the Washington Post. They wrote recently, "China aims not just at eliminating the free speech and virtual free assembly inherent in the Internet, but at turning it into a weapon that can be used against democrats and against democratic societies." Thank you, Mr. Chairman.

Chairman BERMAN. The gentlelady from California, Ambassador Watson, is recognized for 1 minute.

Ms. WATSON. Thank you so much, Mr. Chairman. The Internet is an invaluable tool for expression of information and ideas. Not only does this Internet allow for speedy disbursal, but also reaches scores of people that was previously unimaginable. That is why I feel that Internet security and freedom are so important, and we must be able to protect our constituents and our Government agencies from unwarranted cyber attacks from international players such as China.

Sites such as Twitter and YouTube have provided us with information about unjust acts all around the world, such as the recent videos of election day protests in Iran. These videos provide a window into the world that has previously been closed to us. For that reason, I believe that we must do all we can to protect the freedom of speech on the Internet. Thank you, Mr. Chairman.

Chairman BERMAN. Time of the gentlelady is expired. Who else seeks recognition? The gentleman from New York, Mr. McMahon is recognized for 1 minute.

Mr. MCMAHON. Thank you, Mr. Chairman, and I join those who thank you for scheduling this hearing and having these witnesses come as well. I would just ask that the witnesses, as they address the issue of Internet freedom in China and report on what happened with Google and what is going forward, that they also keep in mind and speak about intellectual property rights and the fact that as we have freedom of information flowing we also respect the rights of those who create music, who create intellectual property, films and the like, because that has become a very valuable good or manufactured thing or commodity that America produces and yet our rights seem to be taken away by those who do that. So I would ask you to focus on that as well as we go forward. Thank you, Mr. Chairman.

Chairman BERMAN. The time of the gentleman is expired. And now we will—oh, the gentleman from New Jersey seeks recognition. Mr. Sires is recognized for 1 minute.

Mr. SIRES. Thank you, Mr. Chairman. As I read this, you know, I am very concerned that the China model may become a model for the rest of the countries that want to stifle free information, and I think it is very important that the negotiations that are going on now do not become a model for all these other countries that want to stifle. I am thinking specifically of Cuba and North Korea. So, you know, you have got your hands full. And I just wanted to make that statement, I know I have a little time, but I will have questions and I want to thank you for being here and thank the chairman for holding this meeting. Thank you.

Chairman BERMAN. The time of the gentleman has expired, and now we are going to introduce and hear from our witnesses. Nicole

Wong is deputy general counsel at Google, working primarily on the company's product and regulatory matters. Prior to joining Google, she was a partner at the law firm of Perkins Coie, where she represented traditional media and new media clients. Ms. Wong also taught media and Internet law courses as an adjunct professor at the University of California at Berkeley, Stanford University, and the University of San Francisco.

Rebecca MacKinnon is a visiting fellow at Princeton University Center for Information Technology Policy, where she is working on a book about China, the Internet, and the future of freedom in the Internet age. She is a cofounder of the Global Voices Online, an Internet blogger's network, and a founding member of the Global Network Initiative, a multi-stakeholder initiative that promotes free expression and privacy around the world.

Dr. Larry Wortzel, serves as a—am I pronouncing that right? Okay—commissioner on the congressionally-appointed U.S.-China Economic and Security Review Commission. Previously, Dr. Wortzel served as vice president for foreign policy and defense studies, and as director of the Asian Studies Center at the Heritage Foundation.

And Robert Holleyman is president and CEO of the Business Software Alliance, an association of the world's leading developers of software, hardware, and Internet technologies. Prior to joining BSA in 1990, Mr. Holleyman spent 8 years on Capitol Hill as legislative director to former U.S. Senator Russell Long, and then as senior counsel for the U.S. Senate Committee on Commerce, Science, and Transportation. We are really very pleased that you folks would come. We apologize for that snow that put this hearing off until now, but all of you working out your schedules to join us today we are very grateful for. Ms. Wong, why don't you lead off?

**STATEMENT OF NICOLE WONG, ESQ., VICE PRESIDENT AND DEPUTY GENERAL COUNSEL, GOOGLE, INC.**

Ms. WONG. Thank you. Chairman Berman, Congressman Smith, and members of the committee, thank you for your continued attention on the issue of Internet freedom. I want to talk to you today about the importance of an open Internet. An open Internet is what allowed a national broadcaster in Venezuela to update daily newscasts on YouTube after Hugo Chavez revoked their broadcasting license because their opinions ran counter to his policies. An open Internet is what ensured the publication of blog reports, photos, and videos of hundreds of Burmese monks being beaten and killed in 2007 even after the government shut down the national media and kicked out foreign journalists.

An open Internet is what brought the protests following the Presidential elections in Iran last summer to all of our attention, even after the government banned foreign journalists, shut down the national media, and disrupted Internet and cell phone service. But the continued power of this medium requires a commitment from citizens, companies, and governments alike. In the last few years, more than 25 countries have blocked Google services, including YouTube and Blogger. The growing problem is consistent with Secretary Clinton's recent speech on Internet freedom when she cited cases from China to Tunisia to Uzbekistan to Vietnam.

For example, our video service YouTube has been blocked in Turkey for 2 years now because of user videos that allegedly insulted Turkishness. In 2009, during elections in Pakistan, the Pakistani Government issued an order to all of its ISPs to block certain opposition videos on YouTube. And of course there is our experience in China, where the last year showed a measurable increase in censorship in every medium including the Internet.

An open Internet, one that continues to fulfill the democratic function of giving voice to individuals, particularly those who speak in dissent, demands that each of us make the right choices to support a free and strong Internet and to resist government censorship and other acts to chill speech even when that decision is hard. As Google's deputy general counsel, part of my job is handling censorship demands from around the world guided by three principles: Maximizing access to information online, notifying users when information has been removed by government demand, and retaining our users' trust by protecting privacy and security.

No examples received more attention than China in recent months. In mid December, we detected a highly sophisticated and targeted attack on our corporate infrastructure, originating from China with a primary but unsuccessful goal to access Gmail accounts. However, it soon became clear that what at first appeared to be solely a security incident was something quite different. Other companies from a range of businesses, finance, technology, media, and chemical, were similarly targeted.

We discovered in our investigation that the accounts of dozens of Gmail users around the world who advocate for human rights in China appear to have been accessed by third parties. Let me be clear that this happened independent of the attack on Google, likely through fishing or malware placed on those users' computers. These circumstances, as well as attempts over the past year to limit free speech online, led us to conclude that we no longer feel comfortable censoring our search results in China. We are currently reviewing our business operations there.

No particular industry, much less any single company, can tackle Internet censorship on its own. Concerted, collective action is needed to promote online free expression and reduce the impact of censorship. We are grateful for law makers, and in particular this committee's leadership, who have urged more companies to join the Global Network Initiative. As a platform for companies, human rights groups, investors, and academics, GNI members commit to standards that respect and protect user rights to privacy and freedom of expression. Additional corporate participation will help the GNI reach its full potential.

Beyond the GNI, every one of us at the grass roots corporate and governmental level should make every effort to maximize access to information online. In particular, government can take some specific steps. First and foremost, the U.S. Government should promote Internet openness as a major plank for our foreign policy. The free flow of information is an important part of diplomacy, foreign assistance, and engagement on human rights. Second, Internet censorship should be part of our trade agenda because it has serious economic implications. It tilts the playing field toward domestic companies and reduces consumer choice. It affects not only U.S.

and global Internet companies, but also hurts businesses in every sector that use the Internet to reach customers.

Third, our Government and governments around the world should be transparent about demands to censor or request information about users or when a network comes under attack. This is a critical part of the democratic process, allowing citizens to hold their governments accountable. Finally, Google supports the commitment of Congress and the administration to provide funds to make sure people who need to access the Internet safely have the right training and tools. I want to thank each of you for your continued leadership in this fight against online censorship. We look forward to working with you to maximize access to information online and promote online free expression around the world.

[The prepared statement of Ms. Wong follows:]

**Testimony of Nicole Wong, Vice President and Deputy General Counsel, Google Inc.**
**Before the U.S. House of Representatives Committee on Foreign Affairs**
**Hearing on "The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade"**
**March 10, 2010**

Chairman Berman, Ranking Member Ros-Lehtinen, and Members of the Committee.

Thank you for bringing attention to the important issue of Internet censorship and for giving me the opportunity to discuss today's global challenges to freedom of expression and access to information online. Internet censorship is a growing global problem that not only raises important human rights concerns, but also creates significant barriers for U.S. companies doing business abroad. As Google's Vice President and Deputy General Counsel, I lead the team that helps Google promote free speech around the world.

The number of governments that routinely censor the Internet has grown from a handful in 2002 to more than 40 countries today. Even in countries that are just beginning to make the Internet available to their citizens, governments are simultaneously building sophisticated tools for blocking and filtering content. Repressive regimes are developing ever more advanced tools to use against dissidents and are sharing censorship tactics across borders. Human rights observers have noted that these governments are "baking in" censorship tools for the Internet rather than chasing after criticism that has already been aired.

The lack of transparency and accountability in blocking and filtering is also a grave concern. Over the last several years, we have seen an increasing number of governments, even democratic ones, choose to blacklist certain sites that they deem harmful without providing any formal oversight of process or meaningful ability to appeal. In the next few years, the Open Net Initiative predicts that we will see more targeted surveillance and increasingly sophisticated malware being used to make the monitoring and documentation of government activity even harder.

But despite these challenges we remain optimistic about the ability of technology to empower individuals and realize the potential for a global Internet community. We believe that maximizing the free flow of information online can help to increase openness and prosperity even in closed societies.

As Google invests in new countries, we look to the following three principles to help us protect online freedom of speech and increase access to information:

- **Access** - maximizing access to information on the Web and tools for the creation of content.
- **Transparency** - notifying users when information has been removed by government demand.
- **Trust** - retaining the trust of our users by protecting their privacy and security from governmental acts intended to chill speech.

With those principles in mind, I would like to address four main issues in my testimony:

First, our situation in China.

Second, the global challenges Google and other U.S. companies face every day from governments who seek to limit free expression online.

Third, the economic implications of censorship.

And finally, the need for governments around the world to do more to reduce Internet censorship and support free expression online.

**China Update**

So let me start by updating you on the situation in China.

We launched Google.cn, our Chinese search engine, in January 2006 in the belief that the benefits of increased access to information for people in China and a more open Internet outweighed our discomfort in agreeing to censor some results. While we have faced challenges, especially in the last 12 to 18 months, we have also had some success.

Google is now the second most popular search engine in China, behind Baidu, and we were the first search engine in China to let users know when results had been removed to comply with Chinese law. Use of our maps, mobile and translation services is growing quickly. And from a business perspective, while our China revenues are still small in the context of our larger business, the last quarter of 2009 was our most successful quarter ever in China.

However, in the last year we have seen increasing attempts to limit free speech on the Web in China. Numerous sites including YouTube, The Guardian, Facebook, Twitter, Blogger and Wikipedia have been blocked, some of them indefinitely. In addition, last June the Chinese government announced that all personal computers sold in China would need to be pre-loaded with software that could be used to filter online content. After a public outcry and pressure from companies, the proposal was later withdrawn.

Most recently, in mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China. What at first appeared to be an

isolated security incident -- albeit a significant one -- turned out upon investigation to be something quite different.

First of all, at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors--were similarly targeted.

Second, we believe that a primary, albeit unsuccessful, goal of the attack was to access Gmail accounts surreptitiously.

Third, we discovered in our investigation that the accounts of dozens of U.S.-, China- and European-based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties. I want to make clear that this happened independent of the security breach to Google, most likely via phishing scams or malware placed on the users' computers.

The attack on our corporate infrastructure and the surveillance it uncovered — as well as attempts over the past year to limit free speech on the Web even further — led us to conclude that we are no longer willing to censor our search results in China and we are currently reviewing our options. This decision is in keeping with our pledge when we launched Google.cn that we will carefully monitor conditions in China, including new laws and other restrictions on our services. As we stated then, if we determine that we are unable to achieve our objectives, we will not hesitate to reconsider our approach to China.

I want to stress that while we know these attacks came from China, we are not prepared to say who is carrying out these attacks. We do know such attacks are violations of China's own laws and we would hope that the Chinese authorities will work with US officials to investigate this matter.

Because this is an ongoing investigation, I am not prepared to say any more about these attacks. However, before moving on to the broader, global challenges we face, I would like to stress that the decision to review our business operations in China was driven by our executives in the United States, without the knowledge or involvement of our employees in China who have worked with dedication and determination to make Google.cn the success it is today.

**Other Global Challenges**

As I mentioned earlier, Google has become a regular focus of governmental efforts to limit individual expression because our technologies and services enable people with Internet connections to speak to a worldwide audience. More than 25 governments have blocked Google services over the past few years.

- YouTube: Since 2007, YouTube has been blocked in at least 13 countries including China, Thailand, Turkey, Pakistan, Morocco, Brazil, Syria, Indonesia, Iran, Saudi Arabia, Myanmar, Bangladesh and Turkmenistan.
- Blogger and Blog*Spot: In the last two years, we have received reports that our blogging platform has been or is being blocked in at least seven countries including China, Spain, India, Pakistan, Iran, Myanmar and Ethiopia.
- Orkut: Our social networking site, Orkut, has been blocked recently in Saudi Arabia, Iran and the United Arab Emirates.

This growing problem was underscored by Secretary of State Hillary Clinton in her recent speech on Internet freedom, when she cited cases from Tunisia to Uzbekistan to Vietnam. Let me just highlight one prominent recent example:

This past June, during the protests that followed the presidential election in Iran, the government of Iran ejected foreign journalists, shut down the national media and disrupted Internet and cell phone service. In spite of this, YouTube and Twitter were cited by traditional journalists and bloggers alike as the best source for firsthand accounts and on-the-scene footage of the protests and violence in Tehran.

With YouTube effectively blocked, Iranians continued to upload videos that documented demonstrations, violent clashes between police and protesters, and other scenes of unrest. You may remember, in particular, the graphic video of Neda Soltan's murder on YouTube that became a testament to the vital role that technology plays in giving a voice to those who once were silenced.

In countries like Iran, online platforms like Twitter, YouTube and Blogger are often the only means for speech to emerge from communities closed off by authoritarian governments - particularly in times of political unrest. So it's imperative for governments, companies, and individuals to do more to ensure that the Internet continues to be a powerful medium for expressing political opinions, religious views and other core speech without restriction.

**Economic Implications**

The debate on Internet censorship is, of course, not only about human rights. At issue is the continued economic growth spurred by a free and globally accessible Internet. Barriers to the free flow of information online have significant and serious economic implications: they impose often one-sided restrictions on the services of U.S. and global Internet companies, while also impeding other businesses who depend on the Internet to reach their customers.

When a foreign government pursues censorship policies in a manner that favors domestic Internet companies, this goes against basic international trade principles of non-discrimination and maintaining a level playing field. Local competitors gain a

business advantage, and consumers are deprived of the ability to choose the best services for their needs. And when a government disrupts an Internet service in its entirety – e.g., blocking an entire website because of concerns with a handful of user-generated postings – the government is restricting trade well-beyond what would be required even if it had a legitimate public policy justification for the censorship.

Opaque censorship restrictions can also be very damaging to the 'host' nation, because they undermine the rule of law and make it very hard for foreign companies to navigate within the law, which has negative consequences in terms of foreign direct investment.

The U.S. government has taken some positive steps to address the means and effects of censorship through trade tools. The United States Trade Representative has sought explicitly to address some of these issues in trade agreements – most recently, in the U.S.-Korea Free Trade Agreement – and we applaud these efforts. And the Commerce Department and USTR have been helpful in the context of particular incidents we have encountered in the past.

But governments need to develop a full set of new trade rules to address new trade barriers. We encourage further efforts along these lines, by the U.S. government and other governments to redress favoritism shown by some governments for indigenous companies over U.S.-based corporations. We should continue to look for effective ways to address unfair foreign trade barriers in the online world: to use trade agreements, trade tools, and trade diplomacy to promote the free flow of information on the Internet.

**How Governments Can Support Free Expression**

Internet censorship is a challenge that no particular industry -- much less any single company -- can tackle on its own. However, we believe concerted, collective action by governments, companies and individuals can help promote online free expression and reduce the impact of censorship.

As I noted previously, our business is based on the three principles of access, transparency, and retaining the trust of online users. These principles are not exclusive to Google, and there are ways that the public and private sectors can work together to advance them.

First, making every effort at both the grassroots and government level to maximize access to information online. The State Department recently issued a request for proposals on projects to help citizens on the ground access information they would not otherwise be able to share or receive. Google supports the joint commitment of Congress and the Obama Administration to provide funds to groups around the world to make sure people who need to access the Internet safely get the right training and tools. This is a great step forward, and we believe much more can be done to support grassroots organizations that develop technology to combat Internet censorship.

Second, establishing transparency as a norm when governments attempt to censor or request information about users, or even when a company's network comes under attack. This is a critical part of the democratic process, and governments must strike a balance between law enforcement and proper disclosure, allowing citizens to hold their lawmakers accountable. In many cases the cloud of secrecy around cyber attacks only works to the attackers' advantage because it enables them to operate more easily under the radar. Some of the sensible ideas we've heard discussed to improve transparency include: requiring annual company reports on the levels of filtering being complied with and requests for personally identifiable information from government officials; and greater engagement by the U.S. government with countries that censor the Internet, so any company disclosures result in concrete actions by the U.S. government.

Third, retaining users' trust by committing to protect their privacy and security. There is nothing new about governments using surveillance and intimidation tactics to chill speech about uncomfortable ideas. What is new is the growing deployment of online surveillance toward these ends. To be clear, we fully support lawful investigation by government authorities to protect individuals and companies. But we are committed to protecting our users against unlawful and overbroad government demands for their personal information and ensuring the security of our networks. The global trend toward increasing government access to online communications is of great concern and demands serious review and oversight. In addition, the U.S. should push for improved international cooperation to protect user privacy.

We are also grateful for the efforts of lawmakers -- and in particular your leadership Mr. Chairman -- to bring more companies into the Global Network Initiative (GNI). As a platform for companies, human rights groups, investors, and academics, the GNI requires its members to commit to standards that respect and protect user rights to privacy and freedom of expression. Additional corporate participation will help the GNI reach its full potential -- and we look to the Members of this Committee for continued leadership.

And finally, ensuring that the U.S. government makes the issue of Internet openness, including the free flow of information, an important part of foreign policy, trade, development and human rights engagement. This includes prioritizing the issue as a matter of U.S. foreign policy, including in various dialogues that the U.S. government pursues with regimes that are heavy Internet restrictors; using trade tools where possible; and perhaps also making it part of the criteria for receiving development aid. Ultimately, governments that respect the right to online free expression should work together to craft new international rules to better discipline government actions that impede the free flow of information over the Internet. We need forward-looking rules that provide maximum protection against the trade barriers of the new technology era.

On the multilateral human rights front, enforcing and supporting the mechanisms of the International Covenant on Civil and Political Rights and others under the UN system (*e.g.*, the UN Human Rights Committee) to demand accountability from governments

for Internet censorship is helpful. At the very least, these mechanisms can be better used to shine light on government abuses.

**Conclusion**

I would like to conclude by thanking Chairman Berman, Ranking Member Ros-Lehtinen, the members of the House Committee on Foreign Affairs and other Members of Congress who have spoken in support of our actions to highlight the importance of upholding the right to online free expression around the world and the challenges faced by U.S. companies. It is only with the attention and involvement of leaders like yourselves that we can make real progress in the effort to protect these basic human rights. We look forward to working with you and other government officials to find viable solutions to maximize access to information, increase transparency and protect users around the world.

Chairman BERMAN. Thank you very much.

Ms. MacKinnon?

**STATEMENT OF MS. REBECCA MACKINNON, VISITING FELLOW, CENTER FOR INFORMATION TECHNOLOGY POLICY, PRINCETON UNIVERSITY, COFOUNDER OF GLOBAL VOICES ONLINE**

Ms. MACKINNON. Thank you, Mr. Chairman and Mr. Smith, for the chance to testify today and for your leadership on this issue which has already begun to impact the behavior of a number of companies. After describing how authoritarianism is adapting to the Internet in ways that often involve companies, I will offer some policy recommendations. Regimes like China and Iran, and a growing list of others, usually start with the blocking of Web sites, but they also use a range of other tactics outlined in greater detail in my written testimony.

They include cyber attacks against activist Web sites; deletion of online content by Internet companies at government request, which entails taking it off the Internet entirely. Surveillance is used in many countries that don't censor the Internet much if at all. In Egypt, for example, heavy surveillance of Internet users is justified as an anti-terrorism measure, but is also used to harass, identify, and persecute peaceful critics of the regime. And finally there is the use of law enforcement demands in countries where the definition of crime includes political speech, which means that companies end up assisting in the jailing and tracking of activists whether or not they had actually intended to do so at the outset when they entered a market.

So what do we do? At the top of my list of recommendations is corporate responsibility. In the fall of 2008, Google along with Yahoo and Microsoft launched the Global Network Initiative, a code of conduct for free expression and privacy, in conjunction with human rights groups, investors, and academic researchers like myself. The GNI recognizes that no market is without political difficulties or ethical dilemmas. Every company, every product, and every market is different. Therefore, we believe in an approach that combines flexibility with accountability.

Fundamentally, however, it is reasonable to expect that all companies in this sector should acknowledge and seek to mitigate the human rights risks associated with their businesses, just as they and other companies consider environmental risks and labor concerns. Next comes legislation. Law may in fact be needed if companies fail to take voluntary action. However, it is important that any law be sufficiently flexible and global in scope to avoid becoming quickly ineffective or even counterproductive due to rapid technological or geopolitical changes.

Meanwhile, I recommend some immediate steps. First, private right of action. It should be easier for victims to take action in a U.S. court of law when companies assist regimes in violating their rights. Second, we need to incentivize private sector innovation that helps support Internet freedom. Third, we need to continue revising sanctions and export controls. We should make it harder for U.S. companies to sell products and services to regimes with a

clear track record of suppressing peaceful political and religious speech.

However, our laws should not, on the other hand, bar companies from serving those who are risking their lives to peacefully voice dissent. The Treasury Department took an important step this week in issuing export licenses for free services and software to people in Iran, Cuba, and Sudan. Other activists and places like Zimbabwe and Syria are still out in the cold, and there remains the issue of paid services and equipment for individual use that can also help promote freedom of expression.

Technical support: Congress deserves great praise for supporting development of tools and technologies that are helping people get around Internet blocking. But these tools do not counter other tactics regimes are also increasingly using. Our support, therefore, should also include tools and training to help people evade surveillance, detect spyware, and protect against cyber attacks. We also need to help people develop mechanisms to preserve and redistribute censored content that has been taken off the Internet. We should also help with platforms through which citizens around the world can share information and tactics to fight for Internet freedom and empower those individuals.

Finally, Secretary of State Clinton has made it clear that Internet freedom is a core American value and policy priority. In reviving the Global Internet Freedom Task Force, the administration can improve coordination so that the U.S. Government agencies to not inadvertently constrain Internet freedom in the course of pursuing other policy goals.

In conclusion, it is clear that the Internet has brought new challenges to all governments, most companies, and most parents for that matter. Mr. Chairman, I hope this Congress will work to ensure that our cybersecurity solutions, our child protection efforts, economic strategies, and business deals at home and abroad will all be compatible with a free and open global Internet. Thank you.

[The prepared statement of Ms. MacKinnon follows:]

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

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

**Committee on Foreign Affairs**
**United States House of Representatives**

**March 10, 2010**

Thank you, Mr. Chairman, for 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 is informed by my experience as a journalist who has lived under 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 month 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

[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

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. 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. 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 described as 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.

- **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.[7] 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.[8] This happened because Skype delegated law enforcement compliance to its local Chinese partner without sufficient attention to how the compliance was being carried out.

- **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.[9] 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

---

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

[7] 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

[9] *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.

themselves, have over the past few years been victim of increasingly aggressive cyber attacks.[10] 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.[11] 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 – remained offline for more than six weeks.[12] 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.[13]

**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

---

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

[11] "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

[12] "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/

[13] "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

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. In November 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 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.

  With a multi-stakeholder membership including human rights groups, socially responsible investors and academics like myself, the 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. 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. However it is fundamentally reasonable to expect all companies in the ICT sector to acknowledge, seek to mitigate, and be held publicly accountable for the human rights risks and concerns associated with their business. It is also reasonable to expect these 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.

  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 are currently reaching out to a range of other companies, with the expectation that they will prefer the GNI approach to accountability than the alternative: legal measures which will inevitably be more burdensome, less flexible and adaptive to technical innovation or geopolitical changes, and much less able to tailor requirements to the uniqueness of each company's specific technologies and business models.

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 all companies in the ICT sector share varying degrees of human rights risk, even as their business models, technologies, and geographies vary widely. We look forward to working with a range of companies from the ICT sector so that we can ensure that our accountability mechanisms are properly adapted and tailored to their specific products and business models. It is our goal to enable as many companies as possible to join the GNI in the near future. Companies which choose not to join the GNI have an obligation 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:

        - 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.

- 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.[14] The The Treasury Department's Office of Foreign Assets Control is to be applauded for taking an important first step this week in issuing a general license for the export of free personal Internet services and software to Internet users in Iran, Cuba, and Sudan.[15]

- ***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.

---

[14] "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/

[15] "U.S. Hopes Interernet Exports will Help Open Closed Societies," by Mark Landler, New York Times, March 8, 2010 at: http://www.nytimes.com/2010/03/08/world/08export.html

- 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.[16] 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

[16] "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)

censorship system.[17] 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.[18] 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 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."[19] 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.

- **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

[17] "GFW Engineering Team Name List," posted to Google Documents in January 2010 at: http://docs.google.com/View?docid=0Ac8NBXfKcGvqZGR0am1ycGRfMWhyZDljcWY4

[18] "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/

[19] "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

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. Congress can do much to strengthen American 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.

- **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. 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.

Chairman BERMAN. I am tempted to say easier said than done, but I hope we can do that.

Dr. Wortzel?

**STATEMENT OF LARRY M. WORTZEL, PH.D., COMMISSIONER, U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION**

Mr. WORTZEL. Chairman Berman, Mr. Smith, members of the committee, thank you for the opportunity to appear today. The views I will present are my own. They are a product of my service on the U.S.-China Economic and Security Review Commission, decades of service as an Army intelligence officer, and decades of study of China. China is the origin of extensive and malicious cyber activities that target the United States. Our commission, in a contracted report, provided a case study of a penetration into the computer systems of an American high technology company.

The study detailed the way the data was acquired and transferred to an Internet protocol address in China and what institutional and individual actors in China may have been involved. Now I am going to discuss three types of malicious Chinese computer network operations: Those that strengthen political control in China; those that gather economic, military, or technology intelligence and information; and those that reconnoiter, map, and gather targeting information on U.S. military, government, or civil infrastructure networks for later exploitation.

The organizations in China most likely to have gathered the information or attempted to gather information about rights activists during the Google penetrations are those responsible for internal security, repression of the Chinese population, and control over the distribution of information. These are the Ministry of State Security, the Public Security Bureau, and subsidiaries of the Chinese Communist Party such as the Party's Central Propaganda Department.

The second type of malicious activity is intended to gather information of military, technical, scientific, or economic value. Gathering this type of information may speed the development and fielding of weapons, improve technology in sectors of China's industries, while saving time and money in research and development, and compromises valuable intellectual property. The organizations of the Chinese Government with the mission and capability to conduct such activities span military and civilian agencies as well as the state owned companies in China's military industrial complex.

Now, not all cyber-espionage in China is government controlled. There are plenty of cyber-espionage entrepreneurs who operate outside the government and who could be working on behalf of Chinese companies or state run science and technology parts. But let us be candid, when the Department of Justice is prosecuting several espionage cases involving the acquisition by China of defense technologies and military information and the same type of data is being stolen by cyber penetrations, a logical person would conclude that the vast majority of this activity is directed by the Chinese Government.

In the third type of cyber activity, China's intelligence or military services penetrate computers that control our vital infrastructure or our military computer networks, reconnoiter them electronically,

and map or target nodes in the system for future penetration or attack. Malicious code is often left behind to facilitate future entry. Regarding this third type of computer network penetration, General James Cartwright suggested that effects associated with a cyber attack could be in the magnitude of a weapon of mass destruction, and former Director of National Intelligence Mike McConnell recently made a similar comparison.

Now, I believe the government should vigorously monitor and defend our Government computer and critical infrastructure networks. Congress also should put in place legislation that facilitates similar programs for industry. Our Government should work closely with allies and friends to combat malicious cyber activity, and we should ally with like minded nations to keep the worldwide web out of the control of some international body and authoritarian governments such as the one in China that would stop the free exchange of ideas and virtual freedom of association. Thank you for the opportunity to testify, and I will be pleased to respond to any questions the committee may have.

[The prepared statement of Mr. Wortzel follows:]

**China's Approach to Cyber Operations: Implications for the United States**

Testimony before the Committee on Foreign Affairs

House of Representatives

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

By

Larry M. Wortzel

Commissioner
U.S.-China Economic and Security Review Commission

Wednesday, March 10, 2010

Rayburn House Office Building

China's Approach to Cyber Operations: Implications for the United States

Larry M. Wortzel

Chairman Berman, Ranking Member Ros-Lehtinen, Members of the Committee, thank you for the opportunity to appear today to discuss how the People's Republic of China approaches cyber warfare, cyber espionage, and how the United States might respond.

It is a pleasure to appear before you today on an issue of great significance to the United States and, indeed, the world. The views I will present here today are my own. They are a product not only of my service on the U.S.-China Economic and Security Review Commission, but from my service as a military officer with significant background in intelligence and counterintelligence activities as well as decades of study of China.

The attacks on Google that prompted this hearing are the most recent example of a series of penetrations into the computer networks of American companies, departments of the U.S Government, and even some members of Congress.

As the U.S.-China Economic and Security Review Commission has documented in its 2009 *Annual Report to Congress*, "China is the origin of extensive malicious cyber activities that target the United States."[1] Attribution of cyber penetrations and malicious cyber activity is difficult, and even quite sensitive, because if one describes how attribution is achieved, it tells the intruder how to modify its operations and make them more effective.

Our Commission, in a contracted report on "The Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," provided a case study of a multi-day penetration into the computer systems of an American high technology company and how the data acquired was transferred to an Internet protocol address in China.[2] The report also discussed the principal institutional and individual "actors" in Chinese computer network operations as well as the characteristics of network exploitation activities that are frequently attributed to China.

In the case of the Google penetrations, apparently servers at two schools in China, Jiaotong University in Shanghai and Lanxiang Vocational School in Shandong Province, were used in routing the attacks.[3] Still, even if the attacks can be traced to China, it is not clear who ordered the attacks. I want to give you my own views on how, through circumstantial evidence, knowledge of the organizations in China responsible for intelligence, security activities and repression or control of the Chinese population, and logic, one can pick out the most likely actors in some of these Chinese computer networks operations.

I will discuss three types of malicious Chinese computer network operations: Those that strengthen political and economic control in China; those that gather economic, military or technology intelligence and information; and those that reconnoiter, map and gather

targeting information in U.S. military, government, civil infrastructure or corporate networks for later exploitation or attack.

First, skilled computer operators in China routinely exploit systems to gain information about what certain political dissidents may say, how they use the web, and with whom they may communicate. The organizations in China most likely to put the information related to individual accounts belonging to people who may be politically active taken in the Google penetrations to use are those responsible for internal security, repression or control of the Chinese population, and control over the distribution of information. These are the Ministry of State Security, the Public Security Bureau, and organizations of the Chinese Communist Party such as the Party's Central Propaganda Department.[4]

I concede that I cannot prove this beyond a reasonable doubt in a court of law. There may be a group of patriotic hackers in China who just hate criticism of the Communist Party and would take such action. But I believe such persistent, systematic and sophisticated attacks, some of which have taken place in the United States, in China, in Germany, and in the United Kingdom, most likely are state-directed. In addition to the Google attacks, there have been attacks on such religious groups as Falun Gong and on adherents of the Dalai Lama, both of which have been singled out by the Chinese Communist Party leadership for suppression. It is the organs of control and repression in China that need the type of information that was extracted from Google and who most profit from such penetrations.

The second type of malicious activity is designed to gather information of military, technical, scientific or economic value. Gathering this type of information may speed the development and fielding of weapons in China, improve technology in sectors of China's industries while saving time and money in research and development, and often compromises valuable intellectual property. The organizations of the Chinese government with the missions and capabilities to conduct such activities span both military and civilian agencies in China, to include the People's Liberation Army (PLA) Technology Reconnaissance Department (signals intelligence or 3rd Department); the Electronic Countermeasures and Radar Department (4th Department); the Ministry of State Security; and the state-owned companies in China's broad military-industrial complex.[5]

Not all of this cyber espionage may be government controlled.[6] There may be plenty of cyber-espionage "entrepreneurs" in China who operate outside government control that could be working on behalf of Chinese companies or the 54 state-run science and technology parks around the country.

Let us be candid, however. When the Department of Justice is prosecuting several espionage cases involving the acquisition of defense technology or information from US companies or Department of Defense agencies, an unidentified official of the Chinese government is cited as the recipient of the information, and the same type of data is being stolen by cyber penetrations, a logical person would conclude that some of this activity is directed by the Chinese government.

The recent attacks against Google exhibit the traits of both of these types of attacks. Google's investigators discovered that, not only had the "Gmail" accounts of Chinese rights activists been compromised, but Google's most cherished intellectual property--its source code--had been targeted.[7] It is therefore both the organs of control and repression in China, as well as China's technological base, that need the type of information that was extracted from Google and who most profit from the penetrations.

The third type of cyber activity may be the most dangerous for our national security. This is where foreign intelligence or military services penetrate the computers that control our vital national infrastructure or our military, reconnoiter them electronically, and map or target nodes in the systems for future penetration or attack. Malicious code is often left behind to facilitate future entry.

Regarding this third type of computer network penetration by China, General James Cartwright, then Commander of the U.S. Strategic Command (USSTRATCOM) and currently Vice Chairman of the Joint Chiefs of Staff, suggested that "I don't think the [United States] has gotten its head around the issue yet, but I think that we should start to consider that [effects] associated with a cyber attack could, in fact, be in the magnitude of a weapon of mass destruction."[8]

General Cartwright testified before the U.S.-China Economic and Security Review Commission that China is actively engaging in cyber reconnaissance by probing the computer networks of U.S. government agencies as well as private companies.[9] General Cartwright told the Commission that a denial of service attack by China has the potential to cause cataclysmic harm if conducted against the United States on a large scale and could paralyze critical infrastructure or military command and control. China currently is thought by many analysts to have the world's largest denial-of-service capability.[10]

The data collected from these computer reconnaissance campaigns can be used for myriad purposes. Obviously, it has intelligence value for the information that may be extracted. It also helps to identify weak points in the networks. Probes into government systems help a potential adversary to understand how leaders in the United States think and to discover the communication patterns of American government agencies and private companies. General Cartwright testified that this information is akin to that which in times past had to be gathered by human intelligence over a much longer period of time. Computer penetrations also amount to extensions into a different part of the electromagnetic spectrum of warfare and information gathering that had been done by signals intelligence collection. Cartwright went on to say that in today's information environment, the intelligence exfiltration that once took years can be accomplished in a matter of minutes in a single download session.

In a recent editorial, former National Security Agency director and Director of National Intelligence Admiral Mike McConnell reinforced General Cartwright's admonition. Admiral McConnell argued that just as in the Cold War when the United States aimed to protect itself against nuclear attack, today we must endeavor to protect "our power grids,

air and ground transportation, telecommunications, and water filtration systems" against the chaos that could result from successful cyber attacks.[11]

In April 2007, while in China, a delegation of Commissioners met with officers from the PLA's premier strategy research institute, the Academy of Military Sciences. When questioned about cyber attacks, the Chinese military officers noted that scholars hold differing opinions about whether a computer network attack may constitute an act of war. Some argued it meets that definition, but others argued that a network attack alone without corresponding conventional attacks does not constitute an act of war.

However, the PLA officers acknowledged that if a cyber attack targets the military capabilities of another country and does significant damage, conventional counterattacks are warranted. They also noted the frequent difficulty in accurately identifying the source of cyber attacks and argued that the source must be clearly identified before a counterattack could be responsibly launched.

Mr. Chairman, Ranking Member Ros-Lehtinen, computer systems play a crucial role in modern economies today. They are vital links in the transmission of energy, fuel, power, banking and financial data, and transportation systems.[12] They are also key components in our national security.

As important components of our national security, however, they make excellent targets. Our unclassified government and military computer systems also have been penetrated, as discussed in the U.S.-China Economic and Security Review Commission reports cited earlier. Data related to our newest defense systems has been compromised and information therein exfiltrated, probably to China, including "several terabytes of data related to design and electronics systems" of the F35 Lightning II, one of the United States' most advanced fighter planes."[13]

According to an article in the *Wall Street Journal*, a senior U.S. intelligence official told the newspaper that "The Chinese have attempted to map our infrastructure, such as the electrical grid, so have the Russians."[14] The article also cites a former Department of Homeland Security Official, who told the *WSJ* that "the espionage appeared pervasive across the U.S. and doesn't target a particular company or region."

The types of activities discussed the *Wall Street Journal* article are not mere speculation on the part of U.S. officials. Chinese researchers at the Institute of Systems Engineering of Dalian University of Technology published a paper on how to attack a small U.S. power grid sub-network in a way that would cause a cascading failure of the entire U.S. west-coast power grid.[15] Ironically, the two Chinese researchers got access to the power grid vulnerability data from U.S. public information. Two other researchers in China, exploiting academic publications from American researchers, analyzed the shortcoming of computer network attacks and introduced a new network attack platform that could include "viruses, worm classes, and a Trojan Horse logic bomb."[16]

Lieutenant General Liu Jixian, of the PLA Academy of Military Science, writes that the PLA must develop asymmetrical capabilities including space-based information support, and networked-focused 'soft attack,' against potential enemies.[17] Xu Rongsheng, Chief Scientist at the Cyber Security Lab of the Institute for High Energy Physics of the Chinese Academy of Sciences, told a Chinese news reporter that:

> *"Cyber warfare may be carried out in two ways. In wartimes, disrupt and damage the networks of infrastructure facilities, such as power systems, telecommunications systems, and education systems, in a country; or in military engagements, the cyber technology of the military forces can be turned into combat capabilities."*[18]

Other military strategists from China's military academies and schools of warfare theory have suggested that the PLA ought to have the capability to alter information in military command and control or logistics systems to deceive U.S. forces on resupply missions or divert supplies, as well as to be able to paralyze ports and airports by cyber or precision weapon attacks on critical infrastructure.[19]

Simply stated, the Chinese armed forces and the security services take the United States as a potential enemy. Conflict is not a certainty, but cyber operations and cyber intelligence collection are already underway and there are regular attacks on the United States from sites in China.

Chinese People's Liberation Army organizations are being trained and prepared in military doctrine to "expand the types of targets or objectives for armed conflict to command and control systems, communications systems and infrastructure."[20] Military strategist Wang Pufeng argues that "battlefield situations awareness is the core of information age warfare, which means that one must be able to destroy or jam the systems that are fundamental to [an adversary's] situational awareness."[21]

With regard to information warfare, Wang Baocun, one of the leading information warfare specialists in the Chinese military, reminds readers in China that "the global information grid and global command and control systems are fundamental to the American defense system, including global positioning satellites."[22] In other Chinese military publications, there are suggestions that to be successful in information age warfare, one's own military must have certain capabilities and must be able to interfere with an adversary's ability to exploit the results of "reconnaissance, thermal imaging, ballistic missile warning, and radar sensing."[23]

All of this suggests that it is the Chinese military and intelligence services that are behind many of the penetrations of our defense systems. In response, the United States should take measures to strengthen the cyber and critical infrastructure of the nation. Senior officials in the Defense and State Departments should not hesitate to raise with Chinese officials complaints about cyber penetrations or attempts to use computer systems and the World Wide Web to further repress the Chinese people, or to attack people who speak out in other counties about Chinese oppression.

At the same time, we should keep in mind that in some areas of cyber crime, such as credit card theft rings and the theft of banking information, China's law enforcement services have cooperated with the United States. And not all computer-hacking in China is controlled by the government. For certain types of banking and criminal activities, China has prosecuted its hackers.

In the following paragraphs I present some of my own views on cyber defenses and policy for your consideration:

We must monitor and defend our computer systems. Deploying robust intrusion detection systems such as the EINSTEIN 2 and 3 systems to monitor computer network flow and give us real-time alerts about malicious or harmful activity on our government computer systems is crucial to national security.[24] This type of scanning should be expanded to include monitoring activity on critical infrastructure networks and on defense contractors who are working on classified defense programs.

Congress should ensure that the appropriate federal agencies are working with their counterparts in allied and friendly countries to detect and combat malicious cyber activity.

The U.S. government must assist in protecting U.S. critical infrastructure systems and, in fact, has the obligation to do so. The government should not inhibit industry's efforts to protect itself and should help ensure that utilities, banks, and businesses have the tools necessary for cyber defense. Regarding this issue, the National Research Council suggests that private companies (including those that operate the nation's infrastructure) may undertake all the passive defensive actions they see fit, and that the government should provide assistance.[25]

The Critical Infrastructure Protection Act (PL 107-296) created a program that enhances information-sharing between the private sector and government and protects the information that is shared. However, if might be useful to review anti-trust exemptions for companies that share information on infrastructure protection. The Internet Security Alliance has called for such a review.

What is left unresolved in law, however, according to a 2009 National Research Council study, is whether private companies and individuals have the right of self-defense through an active response (a counterattack). The Council suggests a review of the Computer Fraud and Abuse Act, Title 18 USC, Section 1030, with a goal of clarifying provisions of the law that make intentional damaging of any computer connected to the Internet a crime and exploring whether an active response should be criminalized.[26] The National Research Council report also presents an excellent discussion of the costs and benefits associated with any government counterattacks.[27]

It will be impossible for the government to pay for all of the necessary security improvements to the level required by the current threat, especially with the private sector

running so many parts of our nation's critical infrastructure. The assessment of who will foot the bill must be done on a case-by-case basis. However, the government must set minimum standards for protection and if industry fails to implement the appropriate levels of protection, then the government will likely have to intervene and enforce stricter regulations.

Congress could assist in this process by enacting reforms that would allow infrastructure owners to deduct the full cost of security-related spending in the year such expenses are incurred. Allowing industries to write off security spending all at once will reduce the significant costs, thereby improving the all-important bottom line for companies investing in security.

Attacks such as the one on Google, partially intended to control media and target people critical of the government in that Communist "People's Democratic Dictatorship," underscore that it is important to keep the Internet free. United States policy should be to keep the Internet out of the control of some as-yet unnamed United Nations body or commission that can be institutionalized to allow authoritarian states like China to use it to repress their populations or restrict the free flow of ideas.

The State Department and other agencies of the Executive Branch should work with like-minded allies in other countries, human rights organizations and companies to monitor and develop common responses to the use of the Internet for repression.

I support laws like the Patriot Act that permit law enforcement and intelligence agencies to monitor and fight terrorists.

More work needs to be done on in defining when cyber penetrations or attacks amount to acts of war, where the perpetrator knows that a computer network attack may "directly cause destruction and serious injury."[28] Congress should require that the Departments of Defense, State and Justice explore these issues. Congress also should encourage such organizations as the American Bar Association and Federally Funded Research and Development Centers to work on these legal issues.

My view is that the Departments of Defense and State, with allied governments, should develop a declaratory policy on criteria to categorize computer network attacks as a use of force under international law.

The U.S.-China Economic and Security Review Commission, on which I serve, has recommended that Congress examine any agreement involving Internet service providers that addresses pressures from the Chinese government to provide personally identifiable information about Internet users. The Commission also recommended that Congress investigate whether Chinese government press and Internet censorship violates China's obligations as a member of the World Trade Organization.

With regard to China's cyber activities in the United States and the impact on national security, the Commission recommended that Congress assess the effectiveness of and

resourcing for law enforcement, defense and intelligence community initiatives that aim to develop effective and reliable attribution techniques for computer exploitation and computer attacks.

The Commission also recommended that Congress urge the administration to develop measures to deter malicious Chinese cyber activity directed at critical U.S. infrastructure and U.S. government information systems.

Thank you for the opportunity to testify today. I will be pleased to respond to any questions the Committee may pose.

Dr. Larry M. Wortzel is a commissioner on the U.S.-China Economic and Security Review Commission. He was appointed by Republican Leader Boehner. Dr. Wortzel is a retired U.S. Army Colonel. During his 32-year military career, he spent 25 years as an intelligence officer. His operational experience is in signals intelligence collection, human-source intelligence collection, and counterintelligence. Dr. Wortzel served two tours of duty as a military attaché in the American Embassy in the People's Republic of China. He has written three books on China and edited ten other books on the Chinese military. His most recent research and writing has focused on exploiting Chinese military publications on People's Liberation Army doctrine for nuclear warfare, space warfare, and cyber warfare.

---

[1] Quote from Joel Brenner, former director of the National Counterintelligence Executive, Office of the Director of National Intelligence, in U.S.-China Economic and Security Review Commission, *2009 Report to Congress,* 111th Congress, First Session, Washington, DC: U.S. Government Printing Office, November 2009, p. 167. Archived at www.uscc.gov.

[2] *US-China Economic and Security Review Commission Report on the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* an assessment prepared for the Commission by the Northrop Grumman Corporation, Maclean, VA, October 9, 2009. http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

[3] *The Wall Street Journal,* "China Real Time Report," "Hacking Probe Elevates Lanxiang School," February 22, 2010, http://blogs.wsj.com/chinarealtime/2010/02/22/hacking-probe-elevates-lanxiang-school/tab/article/

[4] U.S.-China Economic and Security Review Commission, *2009 Report to Congress,* 111th Congress, First Session, pp. 289-309.

[5] Ibid. See also, *Directory of PRC Military Personalities,* October 2008; Timothy L. Thomas, *Decoding the Virtual Dragon: Critical Evolutions in the Science and Philosophy of China's Information Operations and Military Strategy* (Fort Leavenworth, KS: Foreign Military Studies Office, 2007); Ellis Melvin, "A Study of the Chinese People's Liberation Army Military Region Headquarters Department Technical Reconnaissance Bureau"; James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Roy Kamphausen, David Lai, and Andrew Scobell, eds., *Beyond the Strait: PLA Missions Other Than Taiwan* (Carlisle, PA: Strategic Studies Institute, April 2009); Wang

Zhengde, *Jiedu Wangluo Zhongxin Zhan (Interpretation of Network Centric Warfare)* (Beijing: Guofang Gongye Chubanshe, 2004); Wei Baofu and Zhao Xiaosong, *Junshi Xinxi Youxiu Lun (Theory of Military Information Superiority)* (Beijing: National Defense University Press, 2008); and Larry M. Wortzel, "China Goes on the Cyber-Offensive," *Far Eastern Economic Review*, January/February 2009.

[6] U.S.-China Economic and Security Review Commission, *2009 Report to Congress*, 111th Congress, First Session, Section 3: "China's Human Espionage Activities that Target the United States and the Resulting Impacts on U.S. National Security, pp. 158-162.

[7] Kim Zetter, "Hack of Google, Adobe Conducted Through Zero-Day IE Flaw," *Wired.com*, January 1`4, 2010. http://www.wired.com/threatlevel/2010/01/hack-of-adob/#ixzz0exPw8kuh.

[8] U.S.-China Economic and Security Review Commission, *2007 Report to Congress*, 110th Congress, First Session, Washington, DC: U.S. Government Printing Office, November 2007, pp. 95-96. Archived at www.uscc.gov.

[9] Ibid.

[10] Robert Marquand and Ben Arnoldy, "China's hacking skills in spotlight," *The Seattle Times*, September 16, 2007.

[11] Mike McConnell, "How to win the cyber-war we're losing," *The Washington Post*, February 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

[12] Larry M. Wortzel, Ph.D., *Securing America's Critical Infrastructures: A Top Priority for the Department of Homeland Security*, Heritage Lecture #787, Washington, DC: The Heritage Foundation, May 7, 2003. Available at www.heritage.org See also http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VF9-4VVGGTJ-1&_user=10&_rdoc=1&_fmt=&_orig=search&_sort=d&_docanchor=&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=c9229601b87210270a7c800b9f7f9eab

[13] U.S.-China Economic and Security Review Commission, *2009 Report to Congress*, 111th Congress, First Session, p. 167.

[14] Siobhan Gorman, "Electricity Grid in the U.S. Penetrated by Spies," *The Wall Street Journal*, April 8, 2009, www.onlinewsj.com/Article/sb123911480520409908 5.html

[15] Jian-wei Wang and Li-Li Rong, "Cascade-Based Attack Vulnerability on the US Power Grid," Institute of System Engineering, Dalian University of Technology, China, January 15, 2009, in *Safety Science*, Vol. 47, Issue 10, December 2009, pp. 1332-1336.

[16] Mao Chengpin and Fang Bingbing, South China Normal University, "Research of Attack Taxonomy Based on Network Attack Platform," *Beijing Jisuanji Xitong Yingyong*, Chinese Academy of Science Software Institute, in Open Source Center CPP20090928670001.

[17] Liu Jixian, "Innovation and Development in the Research of Basic Issues of Joint Operations," *China Military Science*, 3-2009, in Open Source Center CPP20090928563001

[18] *Dongfang Zaobao, July 10, 2009*, in Open Source Center CPP20090710045002

[19] Min Zengfu, ed., *Kongjun Junshi Sixiang Gailun (An Introduction to PLA Air Force Military Thought)* (Beijing: Jiefangjun Chubanshe, 2006), pp. 175-176; also see Jiang Yamin Yuan *Zhan (Long Distance Operations)*, Beijing: Military Science Press, 2007.

[20] Zhao Erquan, "Lun Xinxihua Zhanzheng dui Wuzhang Chongtu fa de Shenyaun Sixiang," in Liu Jixian and Liu Zheng, eds., *Xin Jishu Geming yu Junshi Fazhi Jianshe (The New Technical Revolution and Building our Military)* (Beijing: Jiefang Jun Chubanshe, 2005, pp. 498-505.

[21] Shen Weguang, JieXijiang, Ma Ji and Li Jijun, *Zhongguo Xinxi Zhan (China's Information Warfare* (Beijing: Xinhua Press, 2005, p. 82-83.

[22] Ibid. pp. 86-87.

[23] Wei Yufu, and Zhao Xiaosong, *Junshi Xinxi Youxiu Lun*, pp. 287-290.

[24] See Kim Zetter, "U.S. Declassifies Part of Secret Cybersecurity Plan," *Wired*, March 2, 1020, http://www.wired.com/threatlevel/2010/03/us-declassifies-part-of-secret-cybersecurity-plan/

[25] National Research Council, *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: The National Academies Press, 2009), pp. 200-203.

[26] Ibid. pp. 204-212.

[27] Ibid. pp. 239-292.

[28] The National Research Council Report discusses this in Appendix D., pp. 356-358. The Council also cites Michael Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37:885-937, 1999.

Chairman BERMAN. Thank you very much.

Mr. Holleyman. For a second I thought I was in the Judiciary Committee.

**STATEMENT OF MR. ROBERT W. HOLLEYMAN, II, PRESIDENT AND CEO, BUSINESS SOFTWARE ALLIANCE**

Mr. HOLLEYMAN. Exactly, that is a good committee as well. Thank you, Mr. Chairman, for holding this hearing today, and Mr. Smith, other members of this committee. This is certainly a timely and important hearing, and the Business Software Alliance which represents leading companies in the software, hardware, and Internet arena welcomes the opportunity to provide its perspective. A number of the companies and individuals talking today have provided key aspects to today's hearing. I would like to talk about some of the challenges that we face as an industry in ensuring that the Internet is an open platform for communication.

We are proud of the fact that the tools that companies—largely American-based companies—have developed and have deployed that have allowed both the greatest economic opportunity and for individual and personal communication to disseminate around the world. The announcement just earlier this week that you referred to in your opening statement, Mr. Chairman, by the Treasury Department shows just how important it is to get communications tools into the hands of individuals, including in countries with repressive regimes.

And the U.S. has an important role in the area of global cyber technology leadership and cybersecurity leadership. President Obama spoke to that issue in the Cyberspace Policy Review, and the international component of that, and the international leadership by the U.S. is critical. I would like to address today three issues: (1) the legal environments that restrict U.S. technology companies from foreign markets; (2) the tolerance of industrial theft of U.S. intellectual property; and (3) the threat of cyber attacks.

First, let me address the market restrictions we are facing. Some governments are taking steps that would displace American technology from current and, more importantly, future and growing markets by implementing restrictive industrial policies. For example, the Chinese Government is pursuing indigenous innovation policies that are aimed at shutting foreign firms out of the market or compelling them to transfer their intellectual property and relocate their research and development to China.

I was pleased to have an opportunity to testify late last year before Ms. Watson in the first subcommittee hearing that looked at this issue. And, Mr. Chairman, your own letter to the Chinese ambassador making it clear that this issue of indigenous innovation policy as a means of shutting American and other countries' companies out of the market not only in technology but for green development—for the most innovative technology—was an issue that demanded high level attention. Certainly the administration is making it such, but we have not yet achieved significant progress with China.

Late last year, China attempted to mandate that all computers sold in the country had Green Dam filtering software. And again,

as you said in your opening statement, Mr. Chairman, we were one of the industry groups that joined together across continents to call on China to reverse that policy because of its impact on security, privacy, and the free flow of information. Fortunately, the Chinese Government suspended this mandate, but it could return in the future.

Other witnesses have addressed specific laws and policies that impose restrictions on the free flow of information, and some of these policies impede the ability of technology companies to operate in these countries. Both at home and abroad, U.S. companies are bound to follow the laws of the jurisdictions where they do business. In some instances, these laws confront American companies with a difficult binary choice: Stay in the market and comply with local law, or leave. We believe that remaining engaged in those markets is important wherever possible to do so.

Second is the issue of theft of intellectual property. Mr. McMahon mentioned this in his opening comment. This is an important issue in many markets. China is probably the market where it is of the highest importance. This problem is restricting the ability of organizations—of companies operating out of the U.S.—and their workers to access foreign markets, and it harms the U.S. economy. Most software theft occurs when an otherwise legitimate business illegally copies software for its use. When that is repeated millions of times around the world, this conduct has a staggering cumulative effect.

But more importantly, software theft distorts competition and it destroys American jobs. A company that steals productivity software for its use competes unfairly against a company that pays for it. Both enjoy productivity benefits from the software, but only one is bearing the legitimate cost. Which means, for example, that in a country like China, where only 20 percent of the productivity software is paid for, Chinese enterprises are enjoying an unfair advantage over their U.S. competitors who are paying for the licensed software.

So this issue goes way beyond the IP industry, and in this case touches every business that is affected by a high-piracy country. And we believe that the U.S. has to use tough diplomacy and tough trade measures to attack these issues.

And third is the issue of cyber attacks and cyber intrusions, one of the three prongs of this hearing. These intrusions and attacks are preventing the Internet from reaching its full potential, and unfortunately the cyber attacks experienced by Google and other companies as talked about today were not unique.

In this era of increased interconnectedness, having commercial security practices as well as government attention to cybersecurity is vital to our economic and national security. Our companies are also among the leaders in building and implementing cyber technology. We support the administration's ambitious international cybersecurity strategy, and this has to be an international priority. No one country can do it alone. In my written statement I have listed seven steps that we would recommend for the U.S. and for any country to look at as a matter of law and working with the private sector to enhance cybersecurity.

Let me simply say in conclusion, Mr. Chairman and Mr. Smith, that the Internet is growing and changing. A majority of Internet users reside outside the U.S., and that majority is growing rapidly. As leaders in Internet technology, U.S. companies have a toe-hold in many of these fastest growing markets. We believe strongly that it is both in U.S. foreign policy interest and U.S. domestic economic interest for U.S. technology companies to remain present in overseas markets as the next generation of the Internet is built out.

And we want to work with this committee, with the Congress and with the government in ensuring that we have the ability as American companies to be the platform that provides these communications and information tools and to fight against the challenges that we face, and we thank you for holding this hearing. I would be happy to answer any questions you may have. Thank you.

[The prepared statement of Mr. Holleyman follows:]

**Testimony of Robert Holleyman**
**President and CEO**
**Business Software Alliance**

**Before the House Committee on Foreign Affairs**

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

March 10, 2010

Good morning. My name is Robert Holleyman. I am the President and CEO of the Business Software Alliance.[1] BSA is an association of the world's leading software and hardware companies. BSA members create approximately 90% of the office productivity software in use in the U.S. and around the world. We appreciate the opportunity to testify today on issues that are important to our member companies.

BSA member companies are committed to fully harnessing the power of the Internet and cyberspace. This is a unique time. Computers and software have transformed our lives at home and abroad. They empower individuals, business and nation states in ways that are now taking shape but are not yet fully shaped. The challenge confronting each of us, and especially this Committee, is ensuring that cyberspace contributes its full measure to the common welfare of all people.

BSA member companies confront three challenges in pursuing this goal. First, intellectual property (IP) theft is a huge and growing problem that harms our entire economy. Promoting and protecting innovation is vital to the software and IT industries. IP laws by purpose and design provide incentives to create and innovate. Countries that tolerate the theft of intellectual property are killing innovation. They are also engaging in unfair trade practices that harm our country by robbing us of much-needed jobs. While the US has taken a leadership role in combating theft of intellectual property, the problem for software remains acute and persistent. We should take a hard look at both international and domestic laws to determine what can be done.

Second, full utilization of the Internet requires that its shape and contours be determined by ingenuity and the drive to use and share information. Policies that seek to bend these developments to the contours of a specific country's industrial development goals are far more likely to cause impediments. Policies requiring innovation to be done within a country's territory to fully enjoy market access, pose a particular threat of Balkanizing global innovation.

---

[1] The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Altium, Apple, Autodesk, AVG, Bentley Systems, CA, Cadence, Cisco Systems, CNC/Mastercam, Corel, Dassault Systèmes SolidWorks Corporation, Dell, Embarcadero, HP, IBM, Intel, Intuit, Kaspersky Lab, McAfee, Microsoft, Minitab, Parametric Technology Corporation, Quark, Quest Software, Rosetta Stone, SAP, Siemens, Sybase, Symantec, Synopsys, and The MathWorks.

Finally, cyber crime is preventing the Internet from reaching its full and considerable potential. The Internet is at its most basic level about relationships between information providers and users of the information. This relationship is built on mutual trust. And that trust is nourished when there is a sense that the information shared and exchanged is secure from misuse and tampering. Thus, ways to increase trust and security is an indispensable component of sound cyberspace and Internet policy. I urge this Committee and the Congress to take a fresh look at all three challenges.

In my testimony, I will give a brief overview of the business software industry and its role in our economy and society. I will describe how the inaction of national governments in the face of massive theft of intellectual property creates real, immediate threats to American jobs and our economy, and propose measures that can be taken to reduce IP theft. I will then describe the increasing trend towards restricting market access and trade challenges that the software industry faces around the world. These challenges include policies that seek to exclude US and other foreign companies from large segments of the market and compel transfers of research and development and IP. Finally, I will discuss the software industry's commitment to security in cyberspace, the security threats we now confront on the Internet and the specific steps that we recommend the United States and all other countries take to address the problem.

**Overview of the Software Industry**

Software and computers have changed the world in which we live. It has made us more efficient, more productive and more creative. Software and computers deliver better results in dealing with national priorities such as health care, energy, infrastructure, education, and e-government. Software has been at the heart of this technology revolution. Software drives productivity and innovation in almost every economic sector, helping businesses of all sizes perform better in good times and bad. It makes our lives easier, more connected, and more fun at home.

The software industry has also proven to be a remarkable engine for jobs and economic growth. The software and related services sector employed almost 2 million people in the US in 2007 in jobs that, on average, paid 195% of the national average. This sector contributed more than $261 billion to US GDP in 2007, making it the largest of the US copyright industries.

Without question, the software industry's direct contribution to our nation's economic health is significant. That's not the whole story, though. Remember that much of the prosperity that the US enjoyed, beginning in the second half of the '90s, was built on increased productivity. Information technology, including software, has been the essential driver of these productivity gains.

Software also lies at the heart of the solutions to a whole host of other challenges we face. Green building design, smart electrical grids and electronic health records are a few of the solutions that depend on software. Today – right now – software is helping to teach essential skills to students, to find the most energy-efficient way to get goods to where they're needed and, quite literally, to heal the sick and injured.

**Intellectual Property Theft**

All of these benefits from a healthy, innovative software industry are imperiled by the simple decision to use software without paying for it. This decision, when repeated by consumers and businesses millions of times throughout the world, has a staggering cumulative effect. One in five copies of PC software in use in this country in 2008, valued at more than $9.1 billion, was stolen. And we have the lowest rate of PC software piracy in the world. Globally, the rate is forty-one percent. That translates into the theft of software worth nearly $53 billion in a single year.

Those who steal software are stealing jobs and tax revenues. A study conducted for BSA by IDC last year found that lowering software piracy rates stimulates the entire IT sector, creating jobs and increasing economic growth and tax revenues. The study concluded that a global 10-point reduction in PC software piracy over four years would deliver an additional 600,000 new jobs, $24 billion in tax revenues, and $141 billion in economic growth.

Reducing piracy delivers indirect benefits as well. Society benefits from new technological innovations. Consumers benefit from more choices and greater competition. Internet users benefit from new ways of communication and expanded creative content made available online. And national economies benefit from enhanced productivity leading to higher standards of living.

The business software industry's most harmful piracy problem traditionally has involved its primary users – large and small corporate, government and other enterprises – that pirate our members' products by making additional copies of software for their own internal usage without authorization. We commonly refer to this activity as "organizational end-user piracy." While we face other forms of piracy, such as pirate CDs and illegal downloads, organizational end-user piracy causes by far the greatest economic harm to our industry.

Organizational end-user piracy occurs in many different ways. In what is perhaps the most typical example, a corporate entity will purchase one licensed copy of software, but will install the program on multiple computers. Other forms of end-user piracy include copying disks for installation and distribution, in violation of license terms; taking advantage of upgrade offers without having a legal copy of the version to be upgraded; acquiring academic or other restricted or non-retail software without a license for commercial use; and swapping disks in or outside the workplace. Client-server overuse – when too many employees on a network have access to or are using a central copy of a program at the same time, whether over a local area network (LAN) or via the Internet – is another common form of end-user piracy.

Organizational end-user piracy goes on in enterprises large and small, public and private. These enterprises receive the productivity benefits that the software provides, while foregoing the expense of licensed copies of the software. Not only do they steal from software producers, in effect these enterprises enjoy an unfair commercial advantage over their law-abiding competitors who must make a choice between paying for software or doing without.

This unfair commercial advantage operates at an international level as well: On average, enterprises in countries with high rates of software piracy are competing unfairly with enterprises from countries with low rates of software piracy. To give a particularly stark example, China's 80 percent software piracy rate means that 4 out of 5 enterprises in China can compete unfairly with enterprises in the US that are paying for the software they use to run their businesses and improve productivity.

I want to urge us all to begin thinking of the problem of intellectual property theft in a different way. The problem is more pervasive, more complex, and more pernicious than it was just a few years ago. Quite frankly, the term "piracy" is outdated. It does not even begin to capture the breadth of the problem. This problem has dire implications for America's future well-being.

There are a number of steps that BSA recommended to Vice President Biden in connection with his December 2009 roundtable discussion on piracy and counterfeiting that the federal government could take to address the problem of IP theft:

<u>Executive Order</u>

The federal government can have a profound effect on software theft through its role as a procurer of goods and services. Under Executive Order 13103 of September 30, 1998, federal agencies must take steps to ensure that they use only legal copies of software. That principle could be extended by executive order to require that federal contractors also use only legal copies of software. Firms that seek to sell goods and services to the US government should certify that their use of software is in compliance with the Copyright Act and relevant license agreements, and that they have controls in place to ensure that this is so. This action by the Administration would establish a standard for other governments to follow.

Legislative Action

The enactment of the PRO-IP Act in 2008 provided the federal government with a range of new tools and resources to coordinate and enhance intellectual property enforcement efforts. BSA supported this important legislation and looks forward to working with you and other officials in its implementations. At this time, we are reviewing with our members potential options for legislative reform beyond those contained in the PRO-IP Act, and will be back in touch with the Committee with any additional recommendations.

We note that there has been a great deal of discussion about the asserted need for a "graduated response" or "three strikes" legislation to address some forms of Internet piracy. This is legislation that would require ISPs to take a series of steps in response to allegations of copyright infringement by their subscribers, ultimately leading to sanctions against subscribers who are deemed repeat infringers.

While we support taking action against repeat offenders, as we have learned from similar efforts in France and elsewhere, it has proved very challenging to find a legislative approach that effectively deters online piracy while respecting users' rights and interests, and safeguarding the myriad legal activities that require access to the Internet. These include such increasingly indispensable activities as online banking, monitoring a child's progress in school, managing one's health care and receiving instantaneous alerts concerning natural disasters and other threats.

Whether in the US or abroad, BSA supports action by ISPs against repeat infringers. We believe that this is responsible action that should be taken on a voluntary basis, and is wholly consistent with existing obligations under law in many jurisdictions. When it comes to government policies that require ISPs to impose sanctions, including potentially the suspension or termination of Internet access, it is important that appropriate safeguards – particularly due process protections – are put into place to protect subscribers. BSA members have articulated a set of key principles on graduated response that we attach for the record.

Cooperation with Trading Partners

Cooperation with our trading partners is essential. As we have noted, software theft is by far the largest form of piracy in dollar terms and by many accounts constitutes 75 percent of worldwide piracy of US copyrighted works. Moreover, because software is integral to economic and business activity, its impact is far greater than the direct losses through theft would suggest.

With these facts in mind, we have four initial recommendations on international initiatives.

First, establishing requirements for the use of legal software by all governments and their contractors would have an immediate positive impact. In virtually every country, the government is the single largest customer of software. Government policies have a substantial effect in shaping local markets, and

establishing requirements for legal use by contractors and governments would have a profound positive effect on deterring corporate and institutional end user piracy.

Second, we urge establishing international regimes to address the unfair trade practices that result from governments' tolerance of software theft, which provides unfair competitive advantages to those companies who operate with stolen software. It is our sense that the trade distortions and job losses that arise from software theft should be subject to specific rules under international trade laws. Thus, we would urge you to examine ways to make such practices subject to WTO disciplines as well as disciplines under bilateral trade agreements and relevant national laws.

Third, move ahead as expeditiously as possible to conclude a meaningful Anti-Counterfeiting Trade Agreement (ACTA). Gaining the commitment of key trading partners to obligations consistent with the strong substantive and enforcement provisions reflected in U.S. law and practice is itself valuable. Moreover, the potential for ACTA to provide a mechanism for further cooperation among governments in enforcement efforts and the development of best practices offers important opportunities.

Finally, with respect to organized criminal counterfeiting of business software we urge government investment in criminal and Internet enforcement resources to intercept and shut down the illicit counterfeit software trade both domestically and overseas. This should include focus on re-importation of counterfeit software for resale on domestic internet sites.

**Challenges in the China Market: IP Theft and Technology Nationalism**

Although the challenges I have just described are present in many countries around the world, I would like to a say a few words about the challenges BSA members confront in China, to illustrate the point.

China is a critically important market for BSA companies. It is already the second largest market in the world for personal computers, and it is growing much faster than developed markets like the US, Europe and Japan. BSA companies are fully committed to the China market and seek to work cooperatively with the Chinese authorities. Most of our members have a presence in China, and many have made substantial investments there.

But China is a market with real challenges – challenges that act as significant barriers to trade. Pervasive, intractable IP theft (estimated at 80% for the PC software sector) deprives US software companies of literally billions of dollars each year, and allows Chinese enterprises to compete unfairly with businesses here in the US. Government policies on technology and procurement act as a further brake on our companies' ability to do business in China. These are issues that require direct engagement to protect US interests and ensure that China lives up to its responsibilities as an economic power and a member of the global trading community.

In addition to its excessively high level of software piracy, China has pursued several policies over the past year that have an adverse impact on the ability of US and other technology firms to do business there.

China's effort last year to mandate use of specific software to filter Internet content – the so-called "Green Dam" controversy – threatened to play havoc with the increasingly interdependent hardware and software systems that comprise the Internet in China. Fortunately, the government of China reconsidered that policy after intervention by businesses and governments on both sides of the Atlantic and the Pacific.

However, a broader challenge faces our industry from China's increasing efforts to implement policies to promote "indigenous innovation" that discriminate against foreign firms and seek to compel them to transfer IP rights to Chinese ownership.

For example, this past November the Chinese government took steps that will essentially close the government market to US and other non-Chinese providers of software and other innovative technologies. Companies in six critical sectors, including software, telecommunications, and energy-efficient products were given a December 10, 2009 deadline to apply to get on a list of preferred products the Chinese government will buy. The criteria for a product to be listed includes requirements that the product contain IP that was developed and owned in China and that its original trademark be registered in China. We believe that few, if any, US companies will qualify unless they turn over their IP to a Chinese entity. This could amount to a potentially massive transfer of IP, jobs and economic power. Mr. Chairman, that is a step that is not in our national interest or in the interest of US companies.

In December, the Chinese government issued another directive that extends government procurement and other preferences for indigenous products to 18 other industry sectors, including heavy machinery. The scope of these efforts affects US companies across many critical sectors that are vital to US economic growth and job creation. These efforts run counter to Chinese commitments to open trade and investment – commitments they have made in various bilateral fora including last year's summit between President Hu and President Obama. We appreciate the strong letter you sent to the Chinese Ambassador raising concerns about these policies.

While I have highlighted policies related to government procurement, I would note that China's efforts to discriminate against foreign companies and compel IP transfers extends to policies related to patents, standards, information security products and other areas.

We believe these discriminatory policies by the Chinese government require an intensified and coordinated response from the Administration. A few weeks ago, BSA joined with 18 other industry associations from the technology and broader business sectors on a letter to Secretaries Clinton, Geithner and Locke, Attorney General Holder and US Trade Representative Kirk urging the Administration to elevate these issues to a strategic priority in our bilateral economic agenda with China.

**Security in Cyberspace**

BSA member companies are leaders in promoting cyber security. They recognize that electronic commerce, which is so vital to our industry and to the economy as a whole, cannot reach its full potential without the trust of consumers and businesses.

I believe that we can draw several important lessons from the cyber intrusions and attacks experienced by Google. First, this was not a unique event. A broad range of companies, including BSA members, has been and will continue to be targeted for cyber intrusions and attacks. In the realm of cyber crime, cyber industrial espionage and other intrusions and attacks, BSA member companies are on the front lines. This highlights the critical importance of having sound commercial security practices in place. It is not merely a business imperative – it is vital to our nation's economic security.

Second, security in cyberspace is a matter of concern for any country that uses innovative technologies. Security readiness is both a matter of national and economic security. But it is also a matter of good global citizenship in an era of increasing interconnectedness. Governments need to establish both good policies and good practices. There are several steps that BSA recommends.

**First**, governments should enable individuals and companies to deploy the security measures necessary to protect their electronic information and systems. In this fast-paced game of cat and mouse, we must not pin computer users down behind static and rapidly outdated Maginot lines. This means governments should not require the acquisition or deployment of specific products or technologies including specific hardware or software and instead should permit the acquisition and use of internationally-accepted cyber security tools, solutions and approaches. It also means that governments should permit the use and deployment of security measures based on internationally accepted standards. Mandates of specific types of technologies, or domestic standards that diverge from international standards, only serve to weaken protection and diminish trust.

**Second**, governments should institute a legislative or regulatory framework that will provide overall guidance for businesses and consumers with respect to privacy. This can be either a comprehensive data protection framework or sector-specific legislation. Such governmental action will complement other mechanisms such as technological solutions, industry best practices, and consumer education to bring about a safer online environment. Any such framework should be consistent with OECD privacy principles and the APEC privacy framework. It should also require covered entities to develop, implement, maintain and enforce reasonable administrative, technical and physical safeguards, appropriate to the size and complexity of the entity, the nature and scope of its activities, and proportional to the likelihood and severity of the potential harm.

**Third**, governments should require that organizations notify individuals when the security of their personal data has been breached. However, not all breaches should be notified, to avoid creating undue alarm. When a breach of security has created a significant risk that the data will be misused, the affected consumers should be notified, so that they can take mitigation measures. Additionally, such notification requirements should exempt breaches where the affected data had been rendered unusable, unreadable or indecipherable to an unauthorized third party through the use of practices or methods such as encryption, redaction, access controls and other such mechanisms that are widely accepted as effective industry practices or industry standards. To do this in the US, BSA supports H.R. 2221 as passed by the House, and S. 1490 as passed by the Senate Judiciary Committee, both of which adhere to these principles.

**Fourth**, governments are under regular and persistent cyber attack from criminals and hostile nations. Therefore, they should implement best in class security to protect their own computers, networks and systems. For U.S. federal agencies, this means urgently reforming the Federal Information Security Management Act (FISMA). This 2002 law was an important milestone in the effort to elevate information security among the management priorities of federal agencies. However, FISMA has not improved information security as much as it was hoped. Agencies can comply with FISMA and yet still have significant gaps in their actual security, because FISMA only requires that they show they have security processes in place, without ensuring that these measures effectively lead to mitigating the cyber risks that the agency actually faces. Congress needs to reform FISMA, to ensure that agencies have the authority and resources to identify and mitigate the cyber risks they actually face. Senator Carper is putting the finishing touches to his bill – S. 921, the United States Information and Communications Enhancement Act. We believe S. 921 will focus more narrowly on consensual FISMA reform provisions when it moves in the Senate Homeland Security and Governmental Affairs Committee, and if it does we will support it in that form. We understand that the House Oversight and Government Reform Committee is also working on reforming FISMA. There is broad consensus among stakeholders about how best to reform FISMA, and we are optimistic that the Oversight and Government Reform Committee will act on it.

**Fifth**, governments should crack down on cyber crime. BSA urges all governments to consider ratifying the Council of Europe Cyber Crime Convention. This treaty, which the United States ratified in 2006, is the only international instrument that prohibits cyber crime and provides for international law

enforcement cooperation against it. It is a foundational component of international cyber security. To assist countries that may not be ready to ratify the Council of Europe Convention, BSA has drafted a model law that can be used to bring their domestic criminal laws up to international standards. It is important to recognize, however, that laws are insufficient without appropriate enforcement. Governments need to effectively enforce their cyber crime laws and their law enforcement agencies must cooperate with their foreign counterparts, to ensure their territories do not become safe havens for cyber criminals. To do this, countries need dedicated and knowledgeable investigators, prosecutors and judges, with adequate resources, and the ability to hand out deterrent penalties.

**Sixth**, countries should enact legislation or adopt regulatory measures to facilitate the voluntary sharing of cyber security information between the government and private sector (e.g. actionable threat and vulnerability information, or incident response plans). Such voluntary information sharing promotes the protection of critical information infrastructure, most of which is owned and run by the private sector.

And **seventh**, governments need to educate the public – home users, children and small businesses in particular – about "cyber hygiene", "safe" and "ethical" computing. This includes education about software piracy, because a lot of risks to the public come from the use of pirated software. Governments should tap industry resources for such efforts because industry, and the information technology industry in particular, have invested a lot into cyber security education.

These seven recommendations form the core of what we recommend the United States government pursue as its international cyber security strategy.[2] We believe such a strategy should address the full range of cyber security issues. Most importantly, its year-round implementation by the various relevant federal agencies should be led by the White House Cybersecurity Coordinator and be well-resourced.

**Conclusion**

Software contributes profoundly to the world in which we live. It allows us to share, to create and to innovate in ways previously unimaginable. Software-driven productivity strengthens national economies, including our own, and makes them more competitive and more prosperous. Unfortunately, software theft, technology nationalism and cyber crime prevent the software industry from realizing its full potential.

Thank you again for the opportunity to testify here today. I look forward to your questions and to continued dialogue on this important topic in the future.

---

[2] The Cyberspace Policy Review, released by the White House on May 29, 2009, recommended the development of "*U.S. Government positions for an international cybersecurity policy framework*" and strengthening "*our international partnerships to create initiatives that address the full range of activities, policies and opportunities associated with cybersecurity.*" (Cyberspace Policy Review, p. vi, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)

**BSA Position on**
**Appropriate Measures to**
**Deter On-Line Piracy of Content**

On-line piracy presents a serious and immediate threat to software developers as well as other copyright based industries. Too many persons now treat illicit acquisition of copyrighted works on-line as a routine matter, ignoring the fact that they are engaging in illegal acts. But it is important not to lose track of the fact that the vast majority of individuals and businesses use software, computers and the Internet for a myriad of legal and legitimate personal and business reasons.

The current voluntary industry-led approach to developing technologies to address on-line content piracy continues to be effective and mandated use of any such technologies is not justified. Measures taken should be tailored to the content piracy issue identified and Government's role should be to ensure that legal offerings for digital content services are facilitated.

BSA members approach proposed solutions to address on-line content piracy with two objectives:

1. To effectively deter illicit downloading, uploading, making available and use of content; and,
2. To ensure existing technologies function as designed, that innovation and the development of new technologies and services are not obstructed, and that users' enjoyment of software, computers and the Internet is not diminished.

BSA members believe due care must be taken to ensure policies meet both considerations. We believe the following principles provide the basis for achieving this balance.

1. Some anti-piracy content identification and filtering technologies may play a useful role in deterring piracy in some limited cases, but they are not a "silver bullet" solution to piracy. Rather, addressing piracy effectively requires ongoing voluntary inter-industry efforts.

2. In appropriate circumstances, BSA supports:
    a. Automated educational notification mechanisms for alleged online infringers and a requirement for ISPs to preserve evidence of repeated infringements such as a users' IP address to enable anti-piracy court proceedings and administrative anti-piracy procedures or appropriate enforcement actions, subject to appropriate safeguards, including those governing privacy;
    b. The imposition of appropriate sanctions, including blocking a user, blocking a site, and the suspension or termination of Internet service for individual repeat offenders, provided:
        i. Such sanctions against individual repeat offenders shall be based on either:
            1. Breach of contract, i.e., the terms of subscriber's contract with the service provider. (Contractual mechanisms are a helpful and efficient way of dealing with on-line piracy and should be encouraged and widely implemented.)
            or
            2. Through a decision by an administrative or judicial entity, provided such entity gives all parties an opportunity to be heard and present evidence, and that the decision can be appealed before an impartial court. Before an order becomes final, parties shall have the opportunity to have the order stayed pending appeal to courts.

3. When developing steps to address on-line content piracy the following shall also be given due consideration:

    a. The voluntary development and use of anti-piracy content identification and filtering technologies should continue unimpeded: this self-regulatory approach is the effective way to address piracy. The specific technologies themselves should be developed through voluntary processes open to all affected stakeholders, and the results should be based on consensus of the participants.

    b. In specific cases where anti-piracy content identification and filtering technology is used, it should be demonstrated to be robust, renewable, interoperable, free of unintended consequences for existing systems and any other relevant criteria necessary to ensure users experience will not be degraded and the development and deployment of new technologies will not be impeded.

    c. Where it is determined that it is necessary to empower national judicial or administrative entities to require the use of anti-piracy content identification and filtering technologies, such entities shall impose the requirement as a remedy on a case by case basis, in view of the specific facts presented, and after all affected stakeholders have had an opportunity to assess the impact of the specific anti-piracy content identification or filter's use on their technologies, and identified issues have been comprehensively addressed.

4. BSA opposes:
    a. The termination of ISP services or any other sanctions or penalties imposed on alleged infringers without due process and, at a minimum, a right of appeal to a judicial authority, except when such penalties are imposed as a result of a breach of contract with the service provider.
    b. Imposition of broad anti-piracy content identification and filtering technological requirements applicable to all Internet users, or all computers and software used to access the Internet, by legislation, administrative fiat or adjudication.

Chairman BERMAN. Well thank you very much, all of you. A lot of questions here. We may, I know I am going to want to have at least my shot at a second round and if others want to as well. I am going to recognize myself for 5 minutes, and then I am going to turn the chair over to Mr. Sherman while I have a meeting, but we will proceed. The Post this morning talks about Iran blocking foreign domestic Web sites—that is the Washington Post, not the New York Post—Iran blocking foreign domestic Web sites to curb antigovernment activists.

It raises an issue that Ms. MacKinnon touches on in her testimony and that we have been thinking about a lot in terms of the Iran sanctions bill and export control reform. In addition to the Treasury license which was granted this week, what changes are needed to our Iran embargo to help facilitate protection for the dissenters in Iran? And the flip side of this is, are there technologies that sometimes U.S. subsidiaries, sometimes companies located in allied countries, are exporting to Iran that may aid their ability for the government to suppress communication? Do any of you just want to take a crack at that?

Ms. MACKINNON. I am happy to take a crack at beginning, I am sure there will be other thoughts as well. Speaking to Iranian bloggers and activists, members of the green movement in Iran, people raise a number of issues, and they very much welcome the initial steps by the Treasury Department in making it legal now for Google and many other companies to provide access to their free services, but there is concern that Iranian activists, it is still illegal for American web hosting companies to provide them paid web hosting service. So if an Iranian green movement Web site wants to be hosted outside of Iran, they cannot purchase that space on a web hosting service directly because it is illegal for that American company to serve them.

Chairman BERMAN. Illegal because our codification of our embargo?

Ms. MACKINNON. Absolutely.

Chairman BERMAN. So an amendment to that could deal with that problem?

Ms. MACKINNON. Right. And also because this latest step only handles free services, for instance another issue that Iranian activists face is the ability to buy domain names outside of .IR, which is controlled by the government, they can't buy domain names very easily directly from international registrars. So they have to go through third parties, people exiled, and so on, and so what that leads to is that their domain names often get stolen by hackers and others, and it makes them much more vulnerable, it makes it much more difficult for them to run Web sites outside of Iran that are accessible.

Chairman BERMAN. Explain that a second, why would it make it more usually subject to theft?

Ms. MACKINNON. So if you cannot control your account directly.

Chairman BERMAN. I see, all right.

Ms. MACKINNON. You are relying on second or third parties.

Chairman BERMAN. There are intermediaries getting into this transaction.

Ms. MACKINNON. It makes it much harder to maintain control over your domain name. And so there have been some instances lately of green movement Web sites that got hacked, and then their domain names were stolen, but they couldn't easily regain control because they couldn't interact directly with the domain name registrars and so on because it wasn't legal for the domain name registrars to do that. So there are a number of issues like that. Activists also point to the issue of——

Chairman BERMAN. Tell you what, let me interject here only because I am going to run out of time. I am actually quite serious about trying to pursue some specific things we need to do to change our law because I think we are going to have an opportunity to in the Iran legislation, and so I will follow up with you.

Ms. MACKINNON. Right. And so the point is that there are a lot of paid services that individuals need access to in order to really speak out in the way they need to.

Chairman BERMAN. I got it.

Ms. MACKINNON. And also individual equipment, access to satellite phones that enable people to access the Internet through satellite and so on, the individual ability to purchase that.

Chairman BERMAN. I am going to follow up with you; we are going to get the specifics and move on that. In my last 20 seconds, Mr. Holleyman, how come more of your members haven't joined the Global Network Initiative?

Mr. HOLLEYMAN. Mr. Chairman, I appreciate the question. Certainly we have discussed this with a number of our members. The Global Network Initiative, as I understand it, was initially created to deal with companies who were functioning mostly as Internet service providers. And so the three largest American companies working in that area, Google, Microsoft, and Yahoo——

Chairman BERMAN. Mr. Holleyman, I hate to do this to myself, but my time is expired, so we will follow up on it.

Mr. ROHRABACHER. I would ask unanimous consent that the chairman be given an extra 30 seconds so we can hear the answer to that question.

Chairman BERMAN. Okay. Thank you.

Mr. HOLLEYMAN. It was an issue that the GNI was initially started to deal with companies who were working as Internet service providers. There are discussions underway with the executive secretariate and others at the GNI about potentially expanding it to deal with companies in a broader group of technology functions. And many of our companies are part of discussing that, but those who are the ISPs, for whom it was created, are part of that effort. Other companies certainly are working actively today with the U.N. Compact as well, so they are looking at it in a variety of ways.

Chairman BERMAN. My time is expired. I recognize the gentleman from New Jersey, Mr. Smith, for 5 minutes.

Mr. SMITH. Thank you very much, Mr. Chairman. Let me ask a few questions of the panelists, and thank you for your testimony and for your work following the White House decision to support Google's action to no longer censor searches, Microsoft made it very clear that it will stay in China, and it was quoted in Forbes, "We've been quite clear that we are going to operate in China," said Micro-

soft CEO Steve Ballmer. On January 22nd Forbes reports that Ballmer suggested in his speech to oil company executives that "Google's decision to no longer filter out Internet searches objectionable to the Chinese Government was an irrational business decision. The U.S. is the most extreme when it comes to free speech."

Frankly, I find that outrageous. I am not sure how the panel feels about that. When I asked the four top Internet companies, more than just Internet, Microsoft, Cisco, Yahoo, and Google, to testify back in 2006 and it took us months to get them to come voluntarily, which they did, we had that kind of statement from each of those representatives. It was disheartening, both to myself as chair and to Tom Lantos, who was the ranking member. We left no stone unturned in trying to point out the disservice that that did to the human rights activists. And now Mr. Ballmer, with that kind of statement, shows that there has been no learning curve or very little, and I would appreciate any thoughts that any of you might have on that statement which I find unconscionable.

Secondly, Harry Wu had testified that Cisco said that the Chinese Secret Police were sold by Cisco Police Net, which substantially enabled the detection, arrest, torture, and incarceration of political dissidents, labor leaders, and religious people as well. As a matter of fact, Ms. MacKinnon, he quoted your Web site in his testimony. Obviously, much damage has been done. As we all know, with any high tech there always needs to be upgrades, there always need to be technological enhancements, as new products come online.

And the issue, as awful as it exists today, the cyber police are combing the Internet looking for anybody who puts in the word Dalai Lama, Falun Gong, underground Christians, Uighurs, you name it. On the security side as well there are all kinds of mischief being done searching for anybody who has a contrary view to Beijing. What would you suggest we do vis-à-vis a Cisco in order to mitigate even more harm being done? At the end title of our Global Online Freedom Act, we originally had a dual-use effort, to try to stop dual-use products, I should say, that could be abused by police. It is now a feasibility study because several members objected to it, but I just want to ask you if you could, I don't have much time, comment on those two issues first, Ballmer and Cisco.

Ms. WONG. So as a member of the Global Network Initiative with Rebecca and both Yahoo and Microsoft, we were frankly very puzzled by the comments that were reported from Mr. Ballmer, because they are not consistent with the conversations we have been having at the GNI for the last 3 years, and certainly we would never minimize the human rights impact of censorship in China or any other country. We do think that the forum for GNI provides a really important role for companies to talk about, what they are seeing on the ground in all of these countries, and hopefully it continues to have that role.

Mr. SMITH. Ms. MacKinnon?

Ms. MACKINNON. I was very puzzled as well by Mr. Ballmer's statement because I too felt that it really contradicted a lot of the work that other Microsoft executives have been doing in the Global Network Initiative. And it certainly is true that the GNI is not seeking to do a one-size-fits-all, that in all cases you have to do X.

Every business is different, these businesses need to make conscious decisions on their own based on precisely what their products are and precisely what their business relationships are. So we are not saying that Microsoft should follow exactly what Google does in all situations. However, Microsoft at a working level has been trying to implement greater transparency and human rights assessments in their businesses in China and elsewhere. So Mr. Ballmer's statement was indeed extremely puzzling.

Mr. WORTZEL. Businesses mitigate risk often without direct concern for human rights or national security, and that is where some of these export controls come in. But dual-use items, I would just tell you, are very difficult. I mean I had an experience in a plant in China, or a manufacturing facility, that was working on pollution control systems. And I looked inside the router boxes and found routers that were coproduced by a major American defense company and ten miles up the road the partner of that defense company had a Chinese electronic warfare and electronic countermeasures regiment in its yard being outfitted with the same routers, so I would just say it is a difficult problem.

Mr. SMITH. I see I am out of time, but if we could go back in the second round to Cisco and some additional questions.

Mr. SHERMAN [presiding]. Thank you. My first question is for Ms. Wong; it may be a step outside the general scope of these hearings. I stumble across illegal pirated works on the Internet, full Bruce Springsteen albums, entire seasons of current television shows available online, and sometimes they are surrounded by Google ads. Now, I understand that it is Google's policy to prohibit users from displaying Google ads alongside unlawful content, and I would like to know how Google is enforcing that policy. When you get a take-down notice for a copyright or trademark owner, do you automatically remove the ads placed next to the infringing material? And how long does it take for you to remove the illegal material and the advertising?

Ms. WONG. So, of course for both business and legal reasons, we feel very strongly about protection of intellectual property and the removal of illegal content from our systems. We build our systems with both automated processes as well as manual processes to make sure that we do that well. I don't know the specific take-down times that you are asking me for, but I am happy to come back.

Mr. SHERMAN. I am going to ask you to supplement your answer for the record.

Ms. WONG. Sure.

Mr. SHERMAN. But is it your policy that when you have unlawful material, you take down the ads?

Ms. WONG. When we identify unlawful material where our ads are showing, it is our policy to remove them.

Mr. SHERMAN. I will ask you to respond for the record to the more detailed portions of the question. Mr. Holleyman, you asked us to get tough. Businesses are always coming to Congress and asking us to get tough, and then when you ask them for specifics they basically ask that we beg in a louder voice, which is not effective with China. Business communities are totally unwilling to say, Well why don't we have a week where we block our ports to Chi-

nese imports? Are you proposing anything tough or are you like other businesses, business representatives just wanting us to beg?

Mr. HOLLEYMAN. We believe that a record needs to built very quickly that is completely solid in terms of the economic harm that is being caused to the U.S., and particularly in my reference to the unfair subsidies that are effectively existing for companies outside the U.S. who are using illegal software, and we know that there are Members of Congress who are asking for those to be built. And then we think that we need to take appropriate action.

Mr. SHERMAN. Does taking appropriate action actually do anything, or are you just asking us to beg with big stacks of legal documents?

Mr. HOLLEYMAN. No, no, I mean we think——

Mr. SHERMAN. Are you proposing action that would in any way diminish Chinese access to U.S. markets or impose taxes on Chinese goods coming into our markets?

Mr. HOLLEYMAN. We are proposing that the U.S. use the bilateral mechanisms we have and the multilateral through the WTO.

Mr. SHERMAN. I guarantee delay and failure unless you are willing to support, and the business community is ready to support, immediate, you know, action at the ports on the ground, real action. These bilateral, you know, we will throw paper at them, they will throw paper at us, nothing is going to happen. And my next question is rather, you know, requires a technical knowledge of the Internet, and I used to look around the audience for someone with a plastic pocket protector and figure that was the person, but I am looking, I can't find anybody in the audience, so I will address this to Mr. Holleyman unless there is someone else with a greater technical knowledge.

And that is, in a war between a group of software engineers that are trying to build a wall and a group of software engineers who are trying to poke holes in the wall, who has got the upper hand? It would seem to me that you just have to poke one hole in the wall, one way for the word to get around to Chinese citizens as to how to have access to the real Internet. How difficult is it for us to build these holes?

Mr. HOLLEYMAN. Our experience in a whole host of areas is that it is always possible to punch a hole. And whether it is just in general security technology, it is always possible to do it. It is not easy, but it happens. And the converse of that is that we look to build more secure systems in the U.S. to prevent attacks. We know that holes will be punched, but we have to keep building in an arms race to build more secure technology.

Mr. SHERMAN. I see my time is expired. I will recognize the man from California, the outstanding representative Mr. Rohrabacher.

Mr. ROHRABACHER. Thank you, Mr. Chairman. I think what we are discussing today actually goes to the heart of a contradiction, and you can't treat gangsters and tyrants as if they are the same as democratic leaders and honest people and expect there not to be some problem developing. And this is what we are talking about here today. China is a vicious dictatorship. They may well have had a lot of economic reform in the sense that they have had economic progress, but there has been no liberalization whatsoever politically.

And we have our business community, you know, stepping on themselves trying to get over there to make a profit dealing with these gangsters. Now, Mr. Chairman, we have got to come to grips with that. The corporate world isn't going to make these decisions on their own. They are looking to us as representatives of the democratic society that we represent to set the ground rules because they aren't able to do it themselves because stockholders are clamoring for profit et cetera. Google is making an attempt, but again, announcements are one thing, actually implementing policies are another. Let me ask one thing. Are religious groups as well, like the Falun Gong, being discriminated against finding themselves with Internet restrictions in China?

Ms. MACKINNON. I can answer your question about the Falun Gong. Yes, Falun Gong material is heavily censored on the Chinese Internet.

Mr. ROHRABACHER. So Falun Gong, the Uighurs we know are, the Tibetan Buddhists are. So we could say that if religion manifests itself in some actual power in a society, we have got a regime that is willing to use a heavy hand to try to stamp that out or to restrict their abilities to utilize technology in their freedom. I don't know, again the central problem here is that we are trying to treat China as if it is Belgium, and it is not. China is not a democratic country, and we should have different rules.

When we talk about World Trade Organization and MFN, what we are really talking about is trying to get a dictatorship into the same rules that apply to democratic countries. You know, this is the challenge we face, I think it is not one that we can solve. I think that frankly dictatorships do not deserve the same trading rights and the same considerations that we give to democratic countries. As I say, it is the concept of free trade between free people.

At the same time we must make sure that we are siding with the people of China. The people of China, I happen to believe, are our greatest ally in the cause of world peace and democracy. Because if we are going to have world peace and the promotion of freedom in the world, the people of China are on the front line, and what we have to make sure that everybody knows is the people of the United States and our Government and, yes, our corporations through government mandates are on the side of the people of China and not the dictatorship.

Which means that when the companies fell over themselves trying to sell computers to the police of China, I am sorry, yes they could say, Well the police are just a neutral thing, they are just law and order. No it is not. The Gestapo and the police in Nazi Germany were not the same as the police in London or in the United States. So, Mr. Chairman, I am looking forward and I want to congratulate you, Mr. Chairman, and Mr. Smith of course, for this Global Online Freedom Act and some of the really—and we have gotten to the point and to the heart of the matter on this trade issue with China, and I am a proud supporter of the Global Online Freedom Act.

And I would hope, and that is why I wanted you to have an extra 30 seconds to answer that, I would hope corporate America starts making some moral stands in that way too when our Government

is trying to stand up for what this country is all about. If it wasn't for our Government and our country standing up for these principles of freedom, none of your corporations would have the ability to make any money, none. Because we wouldn't have freedom in this country, we wouldn't have a free enterprise system. So it behooves you to sort of perhaps get behind great efforts like this in Congress to stand up for American principles. Thank you very much, Mr. Chairman.

Mr. SHERMAN. Thank you, Mr. Rohrabacher. We have another representative from the great state of California, the great Lynn Woolsey.

Ms. WOOLSEY. Thank you, Mr. Chairman. This is so frustrating. The United States is not a vicious dictatorship, we know that. But we have citizens right here in our own country, including very young folks, kids almost, who can break into our own Department of Defense computer systems and information systems, and do from afar. So is this even possible in this world of ours of so many smart people, so many ways around everything to protect information?

And certainly, you know, there is a difference between protecting information through security and economic bottom line and allowing people to have freedom of speech, I mean they go hand in hand. But when we open up for freedom of speech do we then open up even more for the ability to be hacked? Where do we go with this and what is it costing us and what is the tradeoff? I know that is very big, but that is as technical as I can get. Mr. Holleyman?

Mr. HOLLEYMAN. Ms. Woolsey, thank you for the question. I think we know that as we have opened up the Internet and opened up computing technology we have opened up vast channels for positive information and positive growth. At the same time, that interconnectedness has posed vulnerabilities, and it really is very much in the area of cybersecurity an arms race to build more secure systems because the bad elements, bad actors, whether they are state-supported or individuals, have sophisticated technology.

I was in San Francisco last week with 16,000 people for the RSA Security Conference. Howard Schmidt, who is the President's new Cybersecurity Advisor—the first in the White House—spoke quite well about the steps we need to take to make us more secure. There are billions of dollars that the U.S. is spending, both in working with the private sector but also to build more secure networks in the U.S. and to make sure that we have full cybercapacity.

But at the heart of your question is an anomaly, that the U.S. is the largest source of cyber-criminal activity in the world, and that is because we are the most connected country in terms of our business work, so it is not surprising. China is number two. Germany and France are three and four. So this is ultimately a global problem, it is going to take global solutions, and we will not be able to block the cyber intrusions completely. What we have to do is make sure though that we continue to build the best technology, build private sector solutions, and it is neither one nor the other. We will have more interconnectedness, but through that we will have more vulnerabilities.

Mr. WORTZEL. Ms. Woolsey?

Ms. WOOLSEY. Yes?

Mr. WORTZEL. Let me say that just as the government has tried to approach this through ensuring that on Federal systems you have trusted hardware and trusted software developed here in the United States, there are things you can do, at far higher cost. But if your software research and development, and I am just going to use China, if your software research and development is in China and your hardware is being manufactured, researched, developed, and manufactured in China, and people who do this work in China move freely between companies and government agencies, you are never going to be secure. The best you can do is monitor what goes on on your net.

Ms. WOOLSEY. Ms. MacKinnon?

Ms. MACKINNON. Well, Ms. Woolsey, I think you really do hit the heart of the problem about this balance between the need for security and the need for freedom. And really, you know, this goes back to when our own country was being founded and you had the arguments between Thomas Jefferson and Hamilton about where do you get the right balance between freedom and security in order to have both a secure and adequately free society. And we are now kind of taking that argument from a country level to a global level on the Internet, and how do we get that balance right globally? Because we can't divide it up country by country.

And Mr. Rohrabacher pointed out to the problem of treating markets all like they are Belgium. Part of the problem too is that our technology treats all countries like they are Belgium. So Nokia, for instance, when it sold its equipment to Iran, its equipment by default included a lawful interception gateway, which when implemented in the context of proper judicial oversight over the police and what not, is deemed, you know, was required in Europe for Nokia to include that technology in its phones and in its systems. But you take that into a place like Iran and you have got 1984.

Same with the Calea requirements in American made routers and so on, the communications assistance for law enforcement. There are technical requirements that we build into our equipment on the assumption that this equipment is going to be used in a society that has oversight, but then that equipment is sold into a society where there is no oversight and where crime is defined broadly to include political and religious speech. So how do we prevent that from happening?

Ms. WOOLSEY. You are supposed to tell us. You are the witnesses.

Ms. MACKINNON. Well, it is difficult. We need to be thinking about, you know, the systems that we are building and we are assuming are going to be universally used, how are those systems going to get distorted when they are applied globally, and do we need to rethink what we bake into our technology as a default?

Mr. SHERMAN. I think the time of the gentlelady is expired. We have yet another talented Member from the State of California, the ranking member of the Terrorism, Nonproliferation and Trade Subcommittee, of course the best subcommittee of the full committee, and that is of course Ed Royce.

Mr. ROYCE. Thank you, Mr. Chairman. Dr. Wortzel, in reading your testimony, one thing I think jumps out to all these Californians here today, or should, and that is your coverage of the Chi-

nese researchers at the Institute of Systems Engineering of Dalian University of Technology and their published paper on how to attack a small U.S. power grid subnetwork in a way that would cause a cascading failure of the entire U.S. West Coast power grid. How helpful in terms of that university study.

Also, just reading through your testimony and listening to your remarks, Chinese military officers noted that scholars hold differing opinions about whether a computer network attack may constitute an act of war. They also note the frequent difficulty in accurately identifying the source of cyber attacks and argued that the source must be clearly identified before a counterattack could be responsibly launched.

I am going back to your quote from General James Cartwright, who was commander of the U.S. Strategic Command, and he is currently vice chairman of the Joint Chiefs of Staff. He said, "I don't think the U.S. has gotten its head around the issue yet, but I think that we should start to consider that effects associated with a cyber attack could in fact be in the magnitude of a weapon of mass destruction."

And I would ask you in light of those comments, and in light of the fact, as you say, that China currently is thought by many analysts to have the world's largest denial of service capability and you go through exactly what that would mean, let me ask you this. It was reported that the White House National Security Council downgraded China in our country's intelligence collection priorities from priority 1 to priority 2. In your opinion, is China less of a security threat today than it was last year or the year before, and is the decision to downgrade China wise in your opinion? Commissioner?

Mr. WORTZEL. Mr. Royce, it is and remains, according to the director of National Intelligence, the director of the FBI, the number one intelligence threat to the United States. It is only one of two countries that can put nuclear warheads on the United States, and we have no existing arms control architecture with China. So it should absolutely be the number one priority.

Mr. ROYCE. Thank you, Commissioner. I will also ask you, we have heard reports that the cyber attacks on Google and other countries originated from within China, but officially, many have danced around China's role, or at least the Chinese Government's role in this, right? So for a minute if we were to be frank, were these attacks sponsored by the Chinese Government?

Mr. WORTZEL. I don't believe that the Chinese Government has any interest in how Google fares inside China. They have an interest in making sure that Baidu, which is partially owned by them, does well. So if Google has code stolen, I am not a lawyer, I don't have to argue it in court, I am an intelligence officer, I am going to analyze who could do it, who profits, what might happen. I have very little doubt that is who did it. And with respect to this, the information on rights activists, I couldn't tell you if it was the Ministry of State Security or the Public Security Bureau, but it was the Chinese Government

Mr. ROYCE. Thank you. Thank you. We have heard much on China, I think rightfully so. I am equally concerned on the attacks and the persecution especially of Vietnamese cyber-dissidents.

There the government continues its crackdown on those that blog on democracy and human rights. The Communist government there removes some postings, but more problematic is their resorting to violence in the most extreme cases, and I was wondering, and I think I will ask this of Rebecca MacKinnon from Princeton University's Center for Information Technology Policy, I would ask you if you could speak on how bloggers could evade detection from authorities when they want to talk about free speech. How do you get around that kind of?

Ms. MACKINNON. Well, there are tools, anonymity tools. One is called Tor, which is an open source tool, and there are a number of others, that help you disguise your IP address as you access a Web site. So there are methods, and there is a range of other methods as well that people who have gained instruction and awareness can use. But many people are not sufficiently aware of how to cover their tracks on the Internet, and end up taking one measure but not another measure, end up being under surveillance because they downloaded some software that had spyware in it, and so on.

So it is very difficult to evade detection, although it is possible. But there is also a lot of other issues too related to how social networking services, like Facebook to just give one example among many others, how they handle their privacy policies, and to make sure that not only are they to the liking of American teenagers but that also that American companies with global Internet services have really done a human rights stress test on these services to makes sure that certain security services can't take advantage of them.

Mr. SHERMAN. The time of the gentleman has expired.

Mr. ROYCE. Thank you. I thank all the witnesses.

Mr. SHERMAN. I will point out to the witnesses that the statement that America does not torture applies only to the executive branch; the chair has announced his intention to do a second round. And demonstrating that not all wisdom comes from California, we now have an outstanding member of the committee, the gentleman from New Jersey, Mr. Sires.

Mr. SIRES. Well thank you very much. I was getting a complex, Chris and I. I am just wondering, Ms. Wong, how much negotiating powers does a company like Google have when you have foreign governments that have these sense of policies. I mean do you have any leverage at all?

Ms. WONG. It is a very good question. And as a single company, it is based on your ability to engage that government and hopefully having someone who is reasonable on the other side, and that is certainly not always the case. One of the reasons that we were one of the founding members of the Global Network Initiative is actually to improve our ability to deal with these governments, so that you would have a set of companies that could approach a government about policies and as a united front tell them that you were not willing to do certain types of censorship or not willing to deal with some of their more restrictive laws. But it is very difficult and different in every country.

Mr. SIRES. Well, you know, as I looked at—I am originally from Cuba and I am always very interested in the process there. I mean only last year did they allow cell phones on the island. You can

imagine the government how they restrain information, and now we have a situation where somebody was doling out computers and he is in jail. How does a private company and government work together to prevent this stuff from happening? I mean they could care less.

Ms. WONG. Right. From a company perspective, what we do is do a human rights impact assessment before entering a country, before deciding to put people on the ground. So we will actually look at a country in terms of what is the rule of law, what are their censorship laws like, what are their government surveillance laws like, to know it before going in or offering a product there exactly what we might be in for in terms of dealing with that government or regime. That is one step.

We have had in the past issues where we actually couldn't come to agreement with other governments and actually have found that our Government through the State Department and other areas were extremely helpful in being a partner with us to intercede in those discussions. And that is one of the reasons in my recommendations in my testimony I talk about using this making freedom of expression part of our foreign policy, making it part of our trade agreements, which gives both us and our Government a better platform for having those conversations.

Mr. SIRES. Well thank you very much. Dr. Wortzel, we are in the middle of a big cold war here, and I just wanted your opinion on where you think America is at in terms of awareness of how serious this issue is. I mean we have bad economic times, we have issues that we are working on, but is America really focusing enough on this new cold war that is happening today? This could have repercussions beyond, you know, what we can even think.

Mr. WORTZEL. Well, first of all, it is very different from the Cold War in the sense that we don't have, you know, the containment policy against China. We are heavily engaged. But we are certainly already engaged in a cyber war. We are certainly already engaged in a military competition and space competition, and at the same time we are heavily dependent on each other in trade, banking, and finance. So I think you have to be very careful how you navigate your way through that. I think the public needs to be aware of the threats. Much of what the Congress and the American people thought would happen by getting China into the World Trade Organization and opening normal trade relations with it in terms of democratizing did not occur.

Mr. SIRES. Did not.

Mr. WORTZEL. It did not occur, it did not democratize, it got worse, as a matter of fact. So it has a very free economy, or a reasonably free economy that is growing, but more effective repression. So I think——

Mr. SIRES. And it comes to—I hate to interrupt—but it comes to my point that I hate to see the China model become the model throughout some of these countries.

Mr. WORTZEL. Well, I think you are absolutely right there, and it takes careful export controls and careful controls over what we do in terms of trade.

Mr. SIRES. Thank you very much.

Mr. WORTZEL. Thank you.

Chairman BERMAN. The time of the gentleman is expired. The gentleman from Arkansas, Mr. Boozman, is recognized for 5 minutes.

Mr. BOOZMAN. Thank you, Mr. Chairman. I have had a number of small businesses who have been adversely impacted by unfair business practices as I ventured out into the global market. And then just in general, I know that it has been brought up previously, but I really am concerned, I guess I don't understand the ability for a Chinese counterfeiter to use Google advertising to sell its products, to buy that trademark and purchase the trademark of the company involved and then sell the products.

I think there has been litigation in the past, here in the United States, Geico, American Airlines. But for the small businesses, the people that don't have the deep pockets, the people that don't have the ability to litigate and go through that long process, it is very, very difficult. So my question is, why can't we have the same policy? Don't sell another company's trademark to counterfeiters. I mean I just don't understand that. So if you all could comment on that it would be appreciated. But these are the kind of things that have to be worked out in the future as the world becomes smaller. It just seems very, very unfair, and so if you would comment I would appreciate that.

Ms. WONG. So our trademark policies permit advertisers who come to the Google adware system to advertise based on certain keywords. We actually have a very robust process that is both automated and manual to try and prevent the misuse of trademarks and to assist trademark owners in protecting their rights. Having said that, there is a freedom of expression component on being able to advertise on particular keywords. Take apple for example. An advertiser who wants to advertise on the word apple, we have to be able to detect what they mean, whether they are in competition with the computer or with the fruit. And so that type of process is something that we are working on all the time to improve.

Mr. BOOZMAN. So if a business owner, once they establish that there is a problem, and these things are sometimes very cut and dried, then you do take steps and fix the problem immediately?

Ms. WONG. Yes, we do have both an automated and a full team that is dedicated to resolving those issues.

Mr. BOOZMAN. Okay. Would the rest of you all agree? Mr. Holleyman?

Mr. HOLLEYMAN. Congressman, I can't comment on those specific policies. What I can comment on though is the broader question, which is, each of your constituents, businesses large and small, who have competitors in a high-piracy country like China have a disadvantage against their Chinese competitor who is using the same productivity tools but who, in the case of China, 80 percent of those businesses are not paying for it while your constituents are. And so this is an issue that goes well beyond whether you are in the software industry or the technology industry, but it is unfair competition, and in addition to the specific cases related to ads we need to look at this broader impact that goes to every district, every business in this country.

Ms. MACKINNON. Just briefly, to put this in a broader free expression context as well, there have been some concerns, particu-

larly there have been some discussions about policies and laws in some European jurisdictions, and there is also the ACTA, the Anti-Counterfeiting Trade Act, that is a state secret so we don't know what is really in it. But one of the things that sometimes is advocated by copyright holders, who certainly deserve to have their intellectual property protected, is that greater liability be placed on carriers and platforms to censor and surveil their users in order to prevent copyright theft.

But at the same time when putting those mechanisms in place, this comes back to the law enforcement issue that I was raising earlier, it also gives repressive regimes an extra excuse to surveil and censor and put liability on carriers to surveil and censor for political reasons as well. So we need to make sure that as we are seeking to protect legitimate business interests we are also not providing extra tools for repression because they are sort of dual use in that way. Because a lot of governments justify their censorship and surveillance with the excuse of child protection, law enforcement, and copyright protection.

Mr. BOOZMAN. Thank you, Mr. Chairman.

Chairman BERMAN. In fact, I would ask the gentleman if I could suggest unanimous consent that he have 1 additional minute and ask him if he would yield to me on this issue that he is raising.

Mr. BOOZMAN. Thank you, sir.

Chairman BERMAN. I thank the gentleman for yielding. I actually hear stories that there are people who in the name of freedom of expression think that every potential protection of copyrights or patents or trademarks that is suggested could theoretically and potentially, if taken too far, impinge on first amendment rights and therefore oppose any single and every single effort to protect intellectual property. Have you ever come across such people?

Ms. MACKINNON. All the time.

Chairman BERMAN. Okay.

Ms. MACKINNON. I do not count myself among those people.

Chairman BERMAN. Good.

Ms. MACKINNON. I believe we need to find the right balance. I believe there need to be solutions, we just need to be mindful in grabbing at solutions that we are thinking about the larger context and how some solutions can be misused.

Chairman BERMAN. They can. Thank you. And just, I will take that last 5 seconds. Ms. Wong, could you do me a favor and take a look in the context of Mr. Boozman's questions about the misappropriation of Rosetta Stone's trademark on the Google process? People have come to us about that, and this is a good place to do my case work.

Ms. WONG. I don't have the specific background on it, but I am happy to come back to you.

Chairman BERMAN. Thank you very much. My time is expired. The gentleman from New York, Mr. McMahon.

Mr. MCMAHON. Thank you, Mr. Chairman. And thank you again to the esteemed panel. I had to step out for a while so if I repeat something that may have been touched on, I apologize, but I just wanted to get back to that issue of piracy of intellectual property and what it costs America and how we can deal with it. Ms. Wong, maybe you could start. How does Google approach this, whether it

is films or music and people who use Google to, either in this country or abroad, to pirate intellectual material, what is Google's thoughts on it and what is the strategy for dealing with it both here and abroad?

Ms. WONG. So as a technology company and one with a good deal of important software for us, we absolutely believe in the protection of intellectual property, and we think there is a significant legal infrastructure for protecting intellectual property which we think is appropriate. To Ms. MacKinnon's statement earlier though, we also believe that there has to be a balance. And so part of our reason for being here at this meeting is to talk about the lack of a similar infrastructure for platforms for free expression, because we think that that is actually the area where in the past the legislatures have not paid as much attention. We do believe in the protection of intellectual property. We also believe in the balance that permits a continuing and vibrant platform for free expression.

Mr. MCMAHON. So how will you balance that in China and particular where, you know, estimates are, and I know Congressman Sherman talked about this, but, you know, 82 percent of all software products purchased in China were obtained through intellectual property piracy, many through the Internet of course and through using the Google platform to do it. How can you help us protect that American interest, that vital American interest?

Ms. WONG. Yeah, well this is one of those areas where partnership with our Government is obviously really important. Our experience in China was interesting because we were competing with their homegrown search engine, Baidu, which owes a great deal of its popularity to the free download of licensed music. We recently offered, or last year I guess, started doing our own music download service all with licensed music, and tried to set an example in that way that users we thought would appreciate, you know, legitimate licensed music. That has not yet proven to help us very much in that market, but it is one of the ways that we were trying to make headway in China.

Mr. MCMAHON. Can you do more and can we do more?

Ms. WONG. I think that there probably is room for continuing to look at intellectual property laws as we apply them in China. I know there are ongoing conversations now in terms of the trade agreements that we are dealing with, and we would be happy to give you more thoughts on that following the hearing.

Mr. MCMAHON. Thank you. Mr. Holleyman, would you want to?

Mr. HOLLEYMAN. Thank you, Mr. McMahon. I will add to that. Certainly in a country like China we see $6.7 billion in losses due to piracy, a significant portion of that loss is to U.S. software companies but also to Chinese software companies and to the channel. What I think in all of this though that we need to consider is that the impact of this goes far beyond any individual working in a software- or a copyright-based company or even their partners. In an area like software, what we find is that most of the software piracy in China is not necessarily from a counterfeit copies and not necessarily from downloaded copies of software.

For software, which is the largest copyright industry in the world, is when an otherwise legitimate business may have one or two legal copies but they have duplicated it for 50 or 100 or 1,000

or 2,000 workers. And when that happens, they are getting the productivity benefits for their company, they are selling their products at a cheaper price than people in your districts. And so we have to look at this as something that is first and foremost hurting U.S. companies because we are the leaders in producing copyright works. But it is displacing legitimate sales by U.S. companies in a whole host of industries, and we need to look at that.

Mr. MCMAHON. So it affects our very competitiveness, the competitiveness of the American companies.

Mr. HOLLEYMAN. Absolutely, far beyond any company that sees themselves as an intellectual property-based company.

Mr. MCMAHON. Okay, thank you. Thank you very much, Mr. Chairman, I yield back the remainder of my time.

Chairman BERMAN. The gentleman has yielded back the remainder of his time. The gentleman from Illinois, Mr. Manzullo, ranking member on the Asia, the Pacific and the Global Environment Subcommittee, is recognized for 5 minutes.

Mr. MANZULLO. Thank you, Mr. Chairman. I was tied up in other meetings. I caught portions of the testimony. My question here is to Ms. Wong. I remember my staff, Nien Su, who was fluent in Chinese, and typed in Tiananmen Square on Google.cn, and he was led to an official Chinese site treating it I think as a travel opportunity, tourist opportunity. And then he typed on Google.com Tiananmen Square and got a very robust history of everything that happened there. My question to you is, I know you are in negotiations on censorship, but allowing a little bit of censorship is allowing all of censorship. And my question to you is, what if the Chinese say, "That is it, we are not going to change our policies"; what is Google going to do?

Ms. WONG. Thank you, Congressman, that is a very good question. So let me be really clear. Google is firm in its decision that it will stop censoring for China our search results, and we are working as quickly as possible toward that end. The fact of the matter is that we have hundreds of employees on the ground, some of whom are very dear colleagues of mine, and we do not underestimate the seriousness or the sensitivity of the decision that we have made. So we will stop censoring on our .cn property, the results, but we want to do it in an appropriate and a responsible way. There is——

Mr. MANZULLO. What if China says, "You continue, we'll continue to censor or you are out"?

Ms. WONG. We are not going to change our decision on stopping to censor, not censoring results anymore. So if the option is that we will need to both shutter our .cn property and leave the country, we are prepared to do that.

Mr. MANZULLO. Thank you.

Chairman BERMAN. The gentleman yields back the balance of his time. And the gentleman from Missouri, chairman of the International Organizations, Human Rights and Oversight Subcommittee, Mr. Carnahan, is recognized for 5 minutes.

Mr. CARNAHAN. Thank you, Mr. Chairman, and thank you for holding this hearing on how we can transform our cyberspace policy to advance democracy, security, and trade. First I would like to turn to the Universal Declaration of Human Rights adopted in

1948 under the Truman administration. Article 19 says, "Everyone has a right to freedom of opinion and expression. This right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers."

I think that is a great principle, and certainly the Internet was not around when that concept was really adopted, but certainly it applies here today. And I first want to ask about market share in China. I understand Google's market share has grown from about 15 percent in '06 to about 31 percent today, meanwhile Baidu has increased its market share from about 47 percent over the same time period up to 64 percent today. If Google leaves, and Baidu would be handed an effective monopoly, can you make an economic argument why this is not in China's national interest? And let me direct that to Ms. Wong.

Ms. WONG. Well, I think it clearly is in China's economic interest. As I understand it, after we made our announcement that we would no longer be censoring search results Baidu's stock shot right up, and they are a Nasdaq listed company that does quite well obviously based on their market share. Having said that, consistent with our principles as a company, we felt that we could no longer continue to operate under the regulations in China.

Mr. CARNAHAN. And I applaud your company's principled decision. And let me ask next, to what extent would this decision, if you do leave, stifle competition and innovation? How would such a decision limit the ability of other U.S. businesses to operate and advertise in China? And let me ask Mr. Holleyman about that.

Mr. HOLLEYMAN. Mr. Carnahan, thank you for the question. I think it shows just how important it is that the U.S. Government take this on as an issue and ensure that U.S. companies can compete in various markets fairly and consistent with U.S. values. One of the challenges from the data I have seen is that Baidu is the third largest site for searches globally, behind Google and behind Yahoo and above Microsoft. And so one of the challenges will become as we will be doubling the number of Internet users, does a platform like Baidu become a prominent platform not just in China but, as they have indicated, on a global basis?

And so I would submit that it is more important and it is important for the U.S. Government to make sure that companies like Google and Yahoo and Microsoft and others can do business in a market like China so that as that next generation of Internet is built out it will continue to be based on U.S. companies rather than ceding that next generation to companies like Baidu and others who may not have the same commitments that U.S. companies do.

Mr. CARNAHAN. Great. Any others on the panel want to comment on that? Ms. MacKinnon?

Ms. MACKINNON. Well certainly, you know, China has short term interests and long term interests as well, and there are many people in China who are not necessarily members of the government who argue that in the long run China is really hurting itself by censoring, by stifling information, and that China's long term competitiveness and innovation will be best served by being open. So that there are certainly those who are arguing that as well within China, and whatever we can do to help amplify that point of view

and show that actually there are multiple points of view in China about what best serves their interests, I think would be helpful.

Mr. CARNAHAN. Thank you very much. Mr. Chairman, I yield back the balance of my time.

Chairman BERMAN. The time of the gentleman is expired. And the gentleman from Virginia, Mr. Connolly, is recognized for 5 minutes.

Mr. CONNOLLY. I thank the chair. And thank you to all of the panelists for being here today. I had a bill on the floor, so forgive me for being a little late. It passed unanimously, I am glad to say.

Chairman BERMAN. We want to complement you for your exquisite timing.

Mr. CONNOLLY. Thank you, Mr. Chairman. You know, Iran and China are just two prominent examples of countries that have been moving to control or censor, frankly speech, free speech over the Internet. Anyone on the panel, but what role do you see the private sector taking with regard to freedom of expression overseas? And what role should the private sector take with respect to that set of issues?

Ms. WONG. Well I will start but maybe Rebecca will want to jump in too. I think that the private sector has made a really great step by farming the Global Network Initiative, which is a group of not just companies but also human rights organizations, academics, and socially responsible investors. And I think that having that body both as an area for shared learnings as well as having a unified voice on censorship issues around the world is really important. One of the things that we observed in the last few years is that when we went into a country we would be told by government regulators there, hey the guys down the street are doing this, you need to do it too.

Having a coalition of companies that are in agreement with each other about our principles, and also being able to push back together against a government, is extraordinarily important. Having said that, the importance of having strong leadership in our Government to back us up when we make those decisions to open up channels for communication so that we can have reasonable conversations about those things is extraordinarily important.

Mr. CONNOLLY. Yeah, I think that is a really good point.

Ms. MACKINNON. And just to back that up, that is absolutely true. It took a generation for the private sector to recognize that it had responsibilities in terms of labor practices. It took another generation for the private sector to recognize its environmental responsibilities, and now it is time for the entire ICT sector, information communications and technology sector, to recognize its responsibilities as regard free expression and human rights.

And at the moment there are a few leading companies who have really taken the first step, and it is a learning process now through the Global Network Initiative and through the efforts of this committee and others in Congress, to really help the private sector step up to its responsibilities and figure out how to do that and still be competitive. Because I don't think it is always a binary choice, engage or get out.

I think the lessons of Google, Microsoft, and Yahoo over the past few years since 2006 and the first hearings has been that it is often

about how you engage, that you can make specific choices. As Mr. Smith pointed out, in Vietnam, Yahoo, having learned its lessons in China when it didn't think through how it was going to implement certain services, they thought through in Vietnam, how do we provide blogging services without exposing user data to the police in Vietnam? And so it is about helping companies be more thoughtful about their responsibilities while still doing business.

Mr. CONNOLLY. Good point. And I know the two gentlemen want to respond as well, and maybe in your response I would also like to know how you think the Global Network Initiative might play a role in this as well. Dr. Wortzel?

Mr. WORTZEL. Well, I have followed the Global Network Initiative on the commission, on the China Commission. I think that they are moving along well. I encourage Congress to continue to monitor their progress on what they hope to achieve. But I want to use bribery as kind of an analogy. You know, I don't have this great faith that the private sector is always going to behave well. We have got laws that stop U.S. companies from bribing foreign officials. So I think that, you know, you really do need to look at forms of legislation that may, if things like the Global Network Initiative don't catch on and work, may restrict what they can do and force them to adhere to our values. And I will just end it at that.

Mr. CONNOLLY. You have got the final word, Mr. Holleyman.

Mr. HOLLEYMAN. Thank you, Mr. Connolly. I certainly agree with the sentiments of the other panelists, and we applaud the effort of the Secretariate and the members of the Global Network Initiative to look at potential ways of expanding that beyond the original ISP community with whom it was intended to more companies. And certainly I can't commit any particular company to participating in that, but I know that we have many members who are engaged in part of the work plan and discussion about potential participation as it is broadened.

Mr. CONNOLLY. I thank you all. My time is up. I look forward to this as a continuing dialogue. Thank you, Mr. Chairman.

Chairman BERMAN. Thank you. And the gentleman's time is expired. And, if you don't mind having a slightly later than usual lunch, I would like to open up for a few more questions. No one has screamed, so I recognize myself for 5 minutes.

Dr. Wortzel, a specific and a more general question. The specific question: You talk about our greatest vulnerability coming from China and that we have no arms control agreement with China. What about a cyber-control agreement, a bilateral protocol regulating both countries' behavior in cyberspace? There has been some discussion of this. I would be curious about your comments.

The more general question: It is hard to articulate, but somewhere—there have been times when people in the American Government have been quite sanctimonious about attacking what other governments are doing and seeking to ban them, which if literally applied to our own conduct might affect us. Is there a line here that we need to, things that we do because we think they are—there are probably limitations on what we can talk about here—but things that we do because we think they are essential to our national security interest? And of course we are right and the others aren't, but it is harder to sell that internationally.

Mr. WORTZEL. Well, I wouldn't want to touch on the operations of the cyber-commands inside the U.S. military here, but I think you have hit on a very important point. We have a long history, the United States has a long history of arms control discussions and agreements with the Soviet Union that has led both to tacit acceptance of certain rules of behavior and formal treaties. Our attempts to do the same with the People's Republic of China have pretty well failed. And I have been involved with those directly since 1986.

They won't talk to us about incidents at sea seriously, we had a treaty with the Russians. They won't talk and sit down formally in arms control and nuclear strategy negotiations as a confidence building measure. So even though the Russians today are beginning to talk to the United States about cyber, the Chinese have not reached the point of doing that. But your question is an extremely important one because I think what we have to do is focus on strategies to bring them in, track 2 discussions in academia.

Ensuring that there are international conferences that focus on things like the laws of war and how cyber warfare affects international warfare that they can attend. I think that our war colleges should be encouraging legal papers on these subjects, there are very few out there. And you are going to find Chinese responding to these. So gradually you begin to build up a body of almost common law on what constitutes an act of war, what activities are permissible. And remember that the laws of war were essentially written sometime between the end of World War I and mostly the end of World War II. So there is nothing in there about space warfare and the cyber age. We do need to address that.

Chairman BERMAN. Thank you very much. Mr. Holleyman?

Mr. HOLLEYMAN. Let me add one quick point to that, sort of going beyond it. When the President announced the results of the Cyberspace Policy Review, it was a significant undertaking for the first U.S. President to talk about cyberspace policy ever, reflective of the times. But I will say, while we greeted this with great support, probably the least well-developed prong of that plan relates to international, and to the international framework, the international cooperation, what the U.S. is trying to seek from our allies.

There is a great intent, there is work being done, but looking at the auspices of this committee, I think one of the great contributions you can make is to ensure that there is the support, there is the attention, and there is the participation to make sure that that international prong of Cyberspace Policy Review is at least as robust as the domestic, because we don't have domestic security without having it internationally.

Chairman BERMAN. Okay. I have a couple more questions. Mr. Smith, should I just give myself another 2 minutes and we will do the same for you and Mr. Connolly? Okay. This issue of engaging with these countries that I would designate as Internet repressive, or however you would describe it, or removing ourselves completely—there have been articles about the ability to subvert the firewalls that these governments impose. Is there a particular value here to be in the country promoting, sort of knowing that there are ways to overcome those government firewalls that is less-

ened if you simply extricate yourself from that country? In the end, is there an argument to be made that you can get more information and encourage more communications by staying and hoping that those firewalls can be pierced than by just pulling out completely, or can you do it all from internationally just as easily and therefore you don't need to stay? Ms. MacKinnon?

Ms. MACKINNON. I think there certainly is an argument, and that is why Google went into China initially after much soul searching, and why many people in China including dissidents and activists who I know are worried that Google might pull out, because they are afraid that then the firewall is going to come down on all Google services and that will make it harder for people to have independent conversations and gain outside knowledge.

So there is very much a strong argument, and again why it is important to think about not just the binary engage or disengage but how you go about engaging, because there is great benefit to being there on the ground and to helping people access information. And also because blocking isn't the only part of censorship or the only barrier to free expression. You have removals, you have surveillance and attacks and all kinds of things, which makes it all the harder if you are on the outside.

Ms. WONG. If I could just amplify?

Chairman BERMAN. Well, yes.

Ms. WONG. So our experience prior to going into China and offering a localized domain in 2006 is that we were being regularly blocked in China, wholesale. Probably 10 percent of the time, and much of the time even then we were much slower because of the latency of being outside of the country. That was the initial reason for going into China. We found that when we were there we were not blocked as frequently, we found that we were able to do really innovative things, like we were the first company to start displaying when we had removed search results because of government requirements that we let users know, and that actually has now become an industry standard in China and we think that is good for the transparency to the country.

I don't want to underplay what a difficult decision it has been that we may not be able to continue to provide search results in China from the .cn property. We think we did a lot of good there. There was a study by the journal Nature recently where they surveyed scientists in China, and 80 percent of them use Google for their academic research because we are more comprehensive than the local players. But having said that and in doing the evaluation, we actually just felt that we couldn't continue to do what seems to be a trajectory of increasing political censorship.

Chairman BERMAN. All right. Can I try and squeeze in one more, guys? Okay. Mr. Holleyman talked about these discussions about expanding GNI, and I am curious to what extent, and I guess, Ms. MacKinnon, you are directly involved, you are I guess one of the academic participants in that process. To what extent do you see the prospect for that kind of expansion, to go beyond just the ISPs and bring others who have software and hardware products into this initiative?

Ms. MACKINNON. I think the prospects are strong if the other technology companies make efforts.

Chairman BERMAN. Well, do you see a way in which Congress could incentivize those companies as they go back and forth on this issue to tip in favor of joining?

Ms. MACKINNON. Certainly. I mean different members of the GNI might have different public views on this, but I do think that we wouldn't be where we are today if there hadn't been the threat of legislation in the first place, and so Congress certainly has a role to play there. And one of the objections or the excuses for not joining GNI by some companies is that, well it doesn't fit our business model.

And our response is, look this is meant to be a flexible process, this is not meant to squeeze everybody into completely inappropriate frameworks. The point of this is to help companies, no matter what their business model is, no matter what their specific technology, do the right thing. And so our implementation guidelines and our governance charter and our assessment mechanisms can be adapted to anybody who is willing to engage substantively in joining, but they have to make the first step in engaging substantively and seriously on how they can join.

Chairman BERMAN. You can have elasticity as to business models if they will come inside the tent, basically.

Ms. MACKINNON. That is right.

Chairman BERMAN. All right, I am going to yield back, but I do want to indicate that, from much of the testimony that I had a chance to read before the hearing and discussions, I have in mind some legislation. I want to work closely with Mr. Smith who has his own legislation to see if we can come up with something that invests our Government in playing the role they should be playing and that I think the Secretary, by her speech, indicated a willingness to play in getting it on a government-to-government basis, incentivizing people to join, putting some reasonable kinds of obligations on the companies in terms of this very important issue. And so with that I will yield to the ranking member.

Mr. SMITH. Thank you very much, Mr. Chairman. And, Ms. MacKinnon, I think your point about the threat of legislation causing or inspiring some additional action, the week we had the hearing, the day we had the hearing in February 2006, all of a sudden the State Department announced, and we welcomed it obviously, a task force to being looking at this issue and looking at it hopefully robustly. So I think your point was very well taken. All of your points were excellent. Thank you for your testimony and your work.

Let me just, a couple of questions. Right before the Beijing Olympics, Congressman Frank Wolf and I traveled to Beijing on a human rights mission, we met with underground pastors of churches, most of whom were arrested. We had a prisoners list of 732 prisoners and very precise information about their alleged crimes, which was simply trying to live out the Universal Declaration on Human Rights. Labor leaders, you know, there was a broad list. And we got nowhere with that.

But we went to a cyber cafe while we were there, and we spent huge amount of time, both Mr. Wolf and I, accessing every site we could think of, Radio Free Asia, Voice of America, anything pertaining to the Dalai Lama. I even couldn't get my Web site. All of

it was blocked. I don't know what they thought they were blocking when they were blocking my Web site but it was blocked.

And even when I went to a very esoteric search time, and that was Manfred Nowak—the special rapporteur for torture who is a outstanding U.N. diplomat and, you know, he stands head and shoulders, I believe, above many in terms of the preciseness of his reporting—he had done a scathing report on torture in China. And when I typed in Manfred Nowak, what I got was his report on Guantanamo, not his report on Chinese systematic and pervasive use of torture.

So my fear then, and as it always has been, is that a whole generation of Chinese are precluded accurate information, or at least information that they can make accurate or informed decisions about. And so the censoring issue, that and personally identifiable information are, you know, the two hallmarks of the Global Online Freedom Act, so I do hope we move forward on that and I would welcome any further thoughts you have on that.

One concern that I have that I don't think we focus enough on, when I chaired the Africa Subcommittee, I held two hearings on China's increasingly poisoning role on Africa. The fact that when it comes to good governance, you know, they are net exporters to the U.S., our balance of trade was $228 billion over the last 12 months. They export other things too, and that is a repression model that is being scooped up by the likes of people in Sudan and other places, and other currently existing dictatorships are borrowing, Lukashenko in Belarus and others, the model that has been hand-given to them by the Chinese cyber police.

So my question is, you know, I don't think we have the luxury of time. You know, dictatorships are repressing by the day, if you are in a torture chamber or in a gulag somewhat or the Lao Gai in China, you don't know if you are going to live to the next day. So time is of the essence, we don't have the luxury of delay. And so I would raise the issue, you know, we try to share best practices, the United States and other democracies. They are sharing worst practices, and they are doing it as aggressively as we could possibly imagine in Latin America, in Africa, and elsewhere. So I do think we need a hurry-up offense to make sure that we do much more and we do it effectively.

So if you might want to comment on that, because I do think, you know, if you destroy the dissidents, the Lech Walessas of Poland and all the other great leaders, the Harry Wus, who thankfully at least he is alive and well here but exiled, where is democracy and human rights going to come from? You will cower the generation to remain silent and stay under the radar, and that goes for labor leaders and everything else. So these worst practices, I hope our businesses realize that they are not neutral in this. And it is unwitting I think.

When we had the four members of the four biggest companies here, even though we were all upset about what was happening, my sense was, I think it is unwitting, I don't think they want this to happen, I think it is perhaps naivety and maybe some complicity, but who knows? The firewall busting technology, if you could speak to that. You know, we have appropriated $30 million for that. Our friends in the Falun Gong and others feel that they

have a useful product, maybe you want to speak to whether or not—I mean I see it as a sidebar issue. GOFA and those initiatives, government to government, should be the mainstream, but there are technologies that can evade and hopefully.

And finally on the Cisco, which we didn't get time to answer before, their, you know, Police Net and the kind of technology that Cisco has transferred not just to the police but also to the military is extraordinarily effective in making sure that everyone walks in lockstep with a dictatorship or else. So if you could speak to those issues I would appreciate it. And for the record, Mr. Chairman, I would ask that a letter from Google, and I thank them again for endorsing GOFA, from eleven NGOs, including Amnesty International, Reporters Without Borders, a list of eleven, and Freedom House, be made a part of the record.

Chairman BERMAN. We will, subject to reviewing it to see if there are any terms that we can't include. No—it will be included for the record.

[The information referred to follows:]

Google Inc.
1101 New York Ave. NW
Second Floor
Washington, DC 20005

Main 202 346-1100
Fax 202 346-1101
www.google.com

March 8, 2010

The Honorable Christopher Smith
2373 Rayburn H.O.B
U. S. House of Representatives
Washington, D.C. 20515

Dear Representative Smith:

This letter is to confirm Google's support for global online freedom legislation including the Global Online Freedom Act (H.R. 2271). Our support for GOFA is based on our strong belief that we must work to promote and expand free expression online and that the free flow of information across borders is critical to establishing and protecting our nation's leadership in a 21st Century global economy.

As new technology dissolves borders and carries with it the potential for greater freedom of expression around the world, we believe that governments, companies and individuals must work together to protect basic rights to find and share information on the Internet. Online censorship is a growing global problem. Google has become a regular focus of governmental efforts to limit individual expression because our products enable people with an Internet connection to speak to a worldwide audience and gather knowledge otherwise out of their reach. More than 25 governments have blocked our services outright over the past few years.

The U.S. and other governments that value freedom of expression are strongly positioned to fight these attempts to limit access to information on the Internet. We believe that legislation like GOFA and related policy initiatives, including private sector efforts like the Global Network Initiative, can help companies like ours stand against such censorship. Indeed, one of the most effective elements of GOFA is that it would prompt the U.S. government to directly engage in conversations with other governments and lead robust international efforts to better protect individuals from government persecution and uphold the right to online free expression.

Congress has a strong role to play in advancing free expression online. We are grateful for your leadership and the efforts of other lawmakers who understand the importance of building a framework to address new global challenges to free expression. We have suggestions for further ways in which the bill can accomplish our mutual goals, and will work with you and your staff on those changes. We look forward to Congress addressing online free expression and standing up against government attempts to chill speech and restrict access to information.

Sincerely,

Alan Davidson

*Director of Public Policy for the Americas*

*Google Inc.*

# NGO Joint Statement in Support of H.R. 2271, Global Online Freedom Act of 2009

---

March 8, 2010

**Representative Chris Smith**
Ranking Member, Subcommittee on Africa and Global Health
Ranking Member, Congressional-Executive Commission on China
Ranking Member, Commission on Security and Co-Operation in Europe

Dear Representative Smith,

We write to reaffirm our strong support for your legislation, the new Global Online Freedom Act of 2009 (GOFA). The new GOFA is an important bill which will effectively prevent repressive governments from pressuring or coercing US IT companies to cooperate with them in transforming the Internet into a tool of censorship and surveillance.

The Internet has given people living under repressive governments unprecedented opportunities to communicate with each other and to learn about the outside world in ways that their governments forbid. But repressive governments have developed technologies of repression, and they have sought to make Internet and technology companies cooperate in their repression. China, for example, has coerced Yahoo! to turn over its secret cyber police records of political dissidents who send sensitive information over email. In 2005 one such dissident, Shi Tao, was sentenced to 10 years in prison after being identified by Yahoo. China has also convinced Microsoft to shut down Internet blogs in which Chinese users were criticizing their government, and

persuaded Google to censor its search engine results. Chinese citizens using Google's Chinese search engine now cannot even learn of the existence of information about human rights and democracy on the Internet, including that found on U.S. government supported Web sites such as the Voice of America.

Internet companies argue that people living under repressive governments such as China are better off if U.S. companies are there to influence the development of this medium. We agree – so long as U.S. companies set a higher standard with respect to privacy and free expression than do local providers in these societies. Thus far, and despite the commendable effort to organize the Global Network Initiative, the leading U.S. companies have not been able to do so. But this legislation would help ensure that American Internet companies are forces of increased respect for human rights and not tools of further repression. With the Global Online Freedom Act, when the secret police of a repressive government ask an American Internet company to turn over personally identifying information about a political dissident, that company will have to notify the Attorney General, who will have the authority to order the company not to comply.

Crucially, the bill would make it more difficult for repressive governments to obtain Internet user information from U.S. companies when seeking to punish dissidents or other individuals for exercising their right to free expression, as user data would have to be stored outside countries such as China that use such information to jail its citizens. In addition, the bill prohibits U.S. companies from disclosing to officials of repressive countries such as China personally identifying user information except for legitimate law enforcement purposes. Decisions about what information can be disclosed would be made by the U.S. government, removing this burden from the companies involved.

By moving quickly to pass this bill, Congress would send a clear message that US technology firms cannot be forced to violate international human rights standards. It would signal to people around the world that the United States will act to defend free expression on the Internet.

Thank you for introducing this important legislation and working for its speedy enactment.

Reporters Without Borders
Amnesty International
Human Rights Watch
Wei Jingsheng Foundation
China Information Center
Laogai Research Foundation
International Campaign for Tibet
Uyghur-American Association
China Aid Association
PEN American Center
World Press Freedom Committee

Founded 1941

BOARD OF TRUSTEES

William H. Taft IV
*Chair*

Thomas A. Dine
Ruth Wedgwood
*Vice Chairs*

Walter J. Schloss
*Treasurer*

John Norton Moore
*Secretary*
*Governance and Ethics Officer*

Bette Bao Lord
Max M. Kampelman
*Chairs Emeriti*

Richard Sauber
*Of Counsel*

Kenneth Adelman
Goli Ameri
Susan J. Bennett
James H. Carter
Antonia Cortese
Lee Cullum
Paula J. Dobriansky
Alan P. Dye
Stuart Eizenstat
Carleton S. Fiorina
Sidney Harman
D. Jeffrey Hirschberg
Lionel C. Johnson
John T. Joyce
Kenneth I. Juster
Kathryn Dickey Karol
Farooq Kathwari
Anthony Lake
Lawrence Lessig
Michael Lewan
Jay Mazur
Theodore N. Mirvis
Dalia Mogahed
Alberto Mora
Joshua Muravchik
David Nastro
Andrew Nathan
Diana Villiers Negroponte
Lisa B. Nelson
Mark Palmer
Scott Siff
Arthur Waldron
Richard S. Williamson
Wendell Willkie II
Richard N. Winfield

Jennifer Windsor
*Executive Director*

February 4, 2010

Honorable Chris Smith
U.S. House of Representatives
2373 Rayburn Building
Washington, D.C. 2051

Dear Congressman Smith:

I am writing to express Freedom House's support for the Global Online Freedom Act (GOFA) of 2009, H.R. 2271. GOFA is critical for U.S. efforts to combat internet censorship and to promote freedom of expression online.

Dozens of repressive regimes restrict freedom of expression by deploying censorship technologies, conducting surveillance on internet users, and collecting personal data online to intimidate and prosecute their critics. As documented by congressional hearings and human rights reports, including reports by Freedom House, some of these technologies originated from U.S. companies, and China has exploited personal data on internet users provided by a U.S. company to commit human rights abuses.

GOFA contains several important provisions: it would require U.S. companies to host personal data outside of the reach of Internet-restricting governments; give the Attorney General the authority to deny requests for personal data that might be used to repress dissidents; prevent U.S. companies from blocking access to U.S. government-supported websites; and require U.S. companies to disclose the methods of filtering they use and the content they block at the request of repressive regimes. In addition, GOFA would create an Office of Global Internet Freedom in the State Department and explore the feasibility of introducing export controls on filtering and surveillance technologies to Internet-restricting countries.

While voluntary codes of conduct, such as the Global Network Initiative, are commendable, they are insufficient to shield U.S. companies from pressure to filter content or to turn over personal data on peaceful dissidents. GOFA will provide strong protection to U.S. companies against such pressure, because they will be able to point to the penalties contained in GOFA as reason to rebuff demands for collaboration with internet censors and other violators of human rights.

1301 Connecticut Ave., NW
6th Floor
Washington, DC 20036
Tel: 202.296.5101
Fax: 202.293.2840

120 Wall Street
26th Floor
New York, NY 10005
Tel: 212.514.8040
Fax: 212.514.8055

Falk Miksa utca 30 IV/2
1055 Budapest, Hungary
Tel: 361.354.1230
Fax: 361.354.1233

www.freedomhouse.org

If U.S. companies are open to collaboration in online censorship and surveillance, their presence in internet-restricting countries will do more to harm than promote internet freedom. U.S. companies can only do more to promote than to harm internet freedom if they are required to resist pressure from repressive governments to infringe on privacy protections and free expression online.

Freedom House rarely takes a position on draft legislation before the U.S. Congress. When it has done so, Freedom House has supported bills that were critical to the advancement of human rights globally. The Global Online Freedom Act is such a bill.

I strongly endorse the Global Online Freedom Act and appreciate your continued efforts to advance human rights around the world.

Sincerely,

Jennifer Windsor
Executive Director

Ms. MACKINNON. Well, just, I think you raised a lot of really good points. And I was actually a journalist working for CNN in the '90s when the Internet arrived in China, and we were all very naive, I think, in thinking that, well there is no way that an authoritarian government can survive the Internet. Well, I think China is absolutely the poster child for how authoritarianism does survive the Internet, and that this is a model that many regimes are copying. And Chinese networking companies like Hyawei and ZTE are doing very good business in African and Middle Eastern countries as well.

And so that is one thing, and I remember in the 2006 hearing some of the companies basically were saying things like, well as long as we provide the Internet in China, ultimately in the long run that will do everybody more good, so in the short run there are some consequences but, you know, that is just short run, in the long run we are going to be bringing freedom. And I think what we have learned over the last few years is that it is not that simple, and that the so called collateral damage immediately does matter and needs to be taken seriously, and that companies can be providing Internet access yet at the same time enabling authoritarianism's survival in the Internet age and helping to raise this whole generation of people who don't know what they don't know. And so that is very serious.

And as you say about Cisco, I have had conversations with them and they say, well we are not doing anything illegal, you know, we are selling to police forces like we sell to law enforcement all over the world. And this is a problem not just with Cisco but there are a number of American companies selling biometric technologies that are also being used for law enforcement. And to also just speak very quickly to Mr. Holleyman's point about the next generation Internet and the need for American companies to be at the forefront of that, well China and many other countries also want to be at the forefront of building the next generation of the Internet, which is going to be much more mobile, "Internet of things" and so on.

And we need to make sure that our companies are not enabling and contributing to a next generation Internet that does not allow anonymity, that does not allow for privacy and makes dissent even more difficult than it is becoming today. So this is all the more reason why we need to make sure that companies across a broad spectrum of technology applications and business models are all mindful of what they are doing. And then the filtering technology.

Yes, I know a lot of people in China who are using a range of different tools to get around censorship, and this is certainly something that deserves continued support. There is a challenge that I find that actually many Chinese people, many Chinese Internet users, even though they are aware of these tools, aren't using them. So there is a whole other range of issues about education and community building around these tools. And also the fact that again Internet blocking isn't the whole story with censorship. On the Chinese language Internet a lot of content is just being removed, and so that circumvention tools won't help you with that if the content has been taken down or if a site has been hacked, and the self-censorship that takes place because of surveillance and

so on. So we need a whole range of different tactics along with circumvention to help people conduct free and open conversations without fear.

Mr. HOLLEYMAN. Mr. Smith, I will just comment to Ms. MacKinnon's comment about the next generation Internet. I mean one of the—looking at the title of this hearing, how does cyber policy address issues of democracy, security, trade, as we build to a next generation Internet we will definitely be better as a country if the backbone of that is based on U.S. companies. And we will be more secure, there will be more democratization in the world, and we will have greater economic security.

What we need to do is make sure that we are using the most vigorous abilities of the U.S. Government to make these government-to-government issues to really drive this discussion, and then also to work against things that would make it difficult or impossible for U.S. companies in IT to remain in markets. Because as we move to a marketplace for the Internet that will be dramatically larger than it is today, it would not be in the U.S. foreign policy interest for the platform of that Internet to be based on companies who had their genesis and origin in countries that had restrictive policies.

Mr. SMITH. If I could just one 5-second question? Harry Wu said there were 35,000 cyber police, and that was an estimation in 2006. Do any of you have the number of how many police are deployed to that operation?

Ms. MACKINNON. I don't have a very reliable number. It has become very difficult to quantify because every police department, every kind of military division and so on has people who are involved with Internet, but also a lot of policing of the Internet is actually basically outsourced to private companies, so it is not police doing it but Baidu and many other Chinese companies have entire departments of people whose job it is to monitor and censor content. And so a lot of it is not actually being done by police, it is being done by the private sector.

Mr. WORTZEL. I agree with Ms. MacKinnon. I don't think you are going to get a reliable figure today. Cyber militias have been created, reserve public security people are brought in from universities and businesses, and it is outsourced.

Chairman BERMAN. The gentleman from Virginia will have the last question.

Mr. CONNOLLY. Thank you, Mr. Chairman. With respect to piracy, what is the obligation of search engines like Google and what is the obligation of governments in protecting content providers against piracy and especially links to piratical sights?

Ms. WONG. So Google's policy in terms of search starts with the notion of we want to have the most comprehensive index possible. When you type in a search we want to deliver something that is relevant for you. However, when we become aware of content that is illegal, we do remove those from the search engine and have a process for doing that. I think that that is part of being responsible in terms of showing users as much information as possible but also respecting the rights of intellectual property owners.

Mr. CONNOLLY. But what I am hearing you say, Ms. Wong, is Google acknowledges it has some responsibility when you know a

site is illegally piratical and you are putting a content provider at risk linking to that site, you are going to do something about maybe removing that site, or that link.

Ms. WONG. That is right. It is actually governed by a law passed by this body many years ago, the Digital Millennium Copyright Act. We have a process for receiving claims by the intellectual property holder and to process those claims to remove it upon notice. Under that process then for search engines they are taken out of index.

Mr. CONNOLLY. Thank you. Anyone else? Mr. Holleyman?

Mr. HOLLEYMAN. We think there needs to be a workable mechanism. We do believe certainly that the U.S. foundation—the Digital Millennium Copyright Act—was a solid foundation. We also think that there need to be obligations that companies assume on their own where there are repeat instances of piracy that has been identified, whether they are not simply responding to a complaint from a copyright holder but they are also taking affirmative steps to take down repeat infringers and to prohibit means that would monetize activity associated with piracy.

Mr. CONNOLLY. Thank you very much. And thank you, Mr. Chairman. I yield back.

Chairman BERMAN. Well now that you have opened up that issue, I just want to, I just feel compelled to follow up a little bit here. Actually, Ms. MacKinnon, your testimony originally, your first testimony you submitted before the snow week, had some recommendations regarding intermediary liability. You spoke to that in your testimony today but you didn't include that in your conclusions. But if, let us just talk hypothetically.

Ms. Wong, you have mentioned notice and takedown provisions of the Digital Millennium Copyright Act—but if you could have a pretty darn flawless kind of filter to separate what Mr. Connolly has talked about, or add to that child pornography or other things, from other kinds of content, what is wrong with intermediary liability in that situation? In places particularly where there is an activity that makes you something more than just a sort of automatic conduit? Having changed the nature of this hearing.

Ms. WONG. I think we have seen the dangers of intermediary liability, most recently in a case in Italy that was brought against three of our executives for the alleged violation of invasion of privacy under Italian law.

Chairman BERMAN. We talked about that, right.

Ms. WONG. In which three of our executives were criminally convicted for a video that was uploaded to YouTube. Although, when we got notice from law enforcement that that video existed, it was a cyber bullying video that violated our policies, we took it down within hours. However, our three executives have been convicted in an Italian court.

What that means for a service, of any platform service but for YouTube, where users upload 20 hours of video every minute, the concept that you would prescreen or else be subject to liability means that that platform cannot exist with the robustness that has proven to provide video footage of the protests in Iran, of in Burma. There has to be a way to continue to permit the robustness of that

platform. And a prescreening requirement or intermediary liability for user content I think would dampen that.

Chairman BERMAN. That was not a case where you were sort of promoting and advertising linking to this video, right? I mean this was not, you were not trying to commercially exploit the placement of that particular video.

Ms. WONG. Right.

Chairman BERMAN. What if part of the intermediary liability constrained it only to areas where there was an intermediary's action to essentially promote links?

Ms. WONG. Which means the intermediary or the platform has somehow appropriated or reviewed and decided to commercially use that information.

Chairman BERMAN. Yes.

Ms. WONG. I think that that is different. We have actually tried to——

Chairman BERMAN. Okay, now we have narrowed this down. All right.

Ms. WONG. I think that we have tried to find a thread which actually partners with the content holders. So for example on YouTube we have a content ID process where, we are not in a position to know who that content owner is or what their rights in it might be, but the content holders can identify it for themselves and make a decision to have it monetized, to have claimed or to have it taken down.

Chairman BERMAN. That is right. All right, look, thank you all very much for coming. It has been a very valuable hearing. I would like to get, if you would be willing to take the time, some more specific suggestions on these Iran issues of trying to get out of our export prohibitions the kinds of things that could help there for our legislation. We are in a situation where we could make great use of that information. And with that, the hearing is adjourned.

[Whereupon, at 12:34 p.m., the committee was adjourned.]

# APPENDIX

---

## Material Submitted for the Hearing Record

# FULL COMMITTEE HEARING NOTICE

***Committee on Foreign Affairs***

*U.S. House of Representatives*
*Washington, D.C. 20515-0128*

**Howard L. Berman (D-CA), Chairman**

March 3, 2010

**TO: MEMBERS OF THE COMMITTEE ON FOREIGN AFFAIRS**

You are respectfully requested to attend an OPEN hearing of the Committee on Foreign Affairs, to be held in **Room 2172 of the Rayburn House Office Building**:

**DATE:** Wednesday, March 10, 2010

**TIME:** 10:00 a.m.

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

**WITNESSES:** Nicole Wong, Esq.
Vice President and Deputy General Counsel
Google, Inc.

Ms. Rebecca MacKinnon
Visiting Fellow
Center for Information Technology Policy
Princeton University
Cofounder of Global Voices Online

Mr. Robert W. Holleyman, II
President and CEO
Business Software Alliance

Larry M. Wortzel, Ph.D.
Commissioner
U.S.-China Economic and Security Review Commission

**By Direction of the Chairman**

*The Committee on Foreign Affairs seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202/225-5021 at least four business days in advance of the event, whenever practicable. Questions with regard to special accommodations in general (including availability of Committee materials in alternative formats and assistive listening devices) may be directed to the Committee.*

# COMMITTEE ON FOREIGN AFFAIRS

MINUTES OF FULL COMMITTEE HEARING

**Day** Wednesday **Date** 3/10/10 **Room** 2172 RHOB

**Starting Time** 10:05 A.M. **Ending Time** 12:35 P.M.

**Recesses** ____ (____ to ____)

**Presiding Member(s)**

Howard L. Berman (CA), Chairman; Brad Sherman (CA)

***CHECK ALL OF THE FOLLOWING THAT APPLY:***

**Open Session** ✓
**Executive (closed) Session**
**Televised** ✓

**Electronically Recorded (taped)** ✓
**Stenographic Record** ✓

**TITLE OF HEARING or BILLS FOR MARKUP:** *(Include bill number(s) and title(s) of legislation.)*

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

**COMMITTEE MEMBERS PRESENT:**

See attached

**NON-COMMITTEE MEMBERS PRESENT:**

David Wu (OR)

**HEARING WITNESSES: Same as meeting notice attached? Yes** ✓ **No**
*(If "no", please list below and include title, agency, department, or organization.)*

**STATEMENTS FOR THE RECORD:** *(List any statements submitted for the record.)*

Letters to Rep. Christopher Smith from Google, Inc., Freedom House, Reporters Without Borders and various other Human Rights organizations, regarding H.R. 2271 - Global Online Freedom Act of 2009 - submitted by Rep. Christopher Smith

**ACTIONS TAKEN DURING THE MARKUP:** *(Attach copies of legislation and amendments.)*

**RECORDED VOTES TAKEN (FOR MARKUP):** *(Attach final vote tally sheet listing each member.)*

| Subject | Yeas | Nays | Present | Not Voting |
|---|---|---|---|---|

**TIME SCHEDULED TO RECONVENE** _____
**or**
**TIME ADJOURNED** 12:35 P.M.

Doug Campbell

**Doug Campbell, Deputy Staff Director**

**Attendance - HCFA Full Committee Hearing:**
**The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade**
**Wednesday, March 10, 2010 @ 10:00 a.m., 2172 RHOB**

Howard L. Berman (CA)
Donald Payne (NJ)
Brad Sherman (CA)
Diane E. Watson (CA)
Russ Carnahan (MO)
Albio Sires (NJ)
Gerald E. Connolly (VA)
Michael E. McMahon ( NY)
Lynn C. Woolsey (CA)
Barbara Lee (CA)
Joseph Crowley (NY)
David Scott (GA)
Jim Costa (CA)
***David Wu

Christopher H. Smith (NJ)
Dana Rohrabacher (CA)
Donald Manzullo (IL)
Edward R. Royce (CA)
John Boozman (AR)
Michael T. McCaul (TX)
Bob Inglis (SC)

***= Non-Committee Member

**March 10, 2010**

***Verbatim, as delivered***

## Chairman Berman's opening remarks hearing, "The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security and Trade"

In a recent speech on 21st-Century statecraft, Secretary Clinton said the State Department is realigning its policies and priorities to harness and promote the power of the latest communication tools.

Her remarks illustrate the fact that new means of electronic communication have created both opportunities and challenges for those who formulate our national security and foreign policy.

While many congressional committees have looked at the issues of human rights, defense, and trade in connection with the Internet, it is time for us to consider a comprehensive approach to the increased worldwide use of cyber-technology.

This hearing will address what we're calling the "Google Predicament" because Google's experience over the past couple of months highlights the challenges in developing a cyber-specific foreign policy. The Internet is a useful tool to promote freedom and trade, but in some places it also serves as a means of censorship. It's a boon for U.S. business, but also a source of great vulnerability with respect to U.S. national security. Reconciling these conflicting policy challenges is a key mission for the Administration and, I believe, for this committee.

The latest communication technologies are being put to use to advance democracy and protect human rights. Widespread use of Twitter overcame the Iranian regime's ban on media coverage of last summer's election results and their aftermath. And a graphic video posted on YouTube of a young Iranian woman who was shot and killed during a protest galvanized world opinion, as it gave people an unvarnished look at the crackdown.

The Administration acknowledged the power of these communication tools just this past Monday by granting a general license for the transfer of social networking software to Iran and other repressive nations. This is an important and good step that will foster greater freedom of expression.

But paradoxically, cyber-technology also serves as a weapon of choice for repressive regimes. Under our former chairman, Tom Lantos, this committee examined closely how American companies, however passively, can and do facilitate censorship. Our colleague Chris Smith has also been very active in advancing the discussion of this subject.

The notion that American companies can heedlessly supply their software, routers, and information to governments that use them for repressive purposes is untenable. But preventing companies from engaging in trade with countries ruled by those repressive governments is equally untenable, for it would deny billions of people the ability to access the very information needed to support their resistance.

When it comes to human rights, there must be a way to balance the benefits of cyber-technology with its very real potential harms. A voluntary organization known as the Global Network Initiative, made up of human rights organizations and various companies, works directly on this

issue. Regrettably, many companies have failed to join. As a result, we may consider legislation to address this issue. Providers of technology need to step up.

American companies did just that last year when Beijing mandated installation of the Green Dam-Youth Escort Software on all computers sold in China. This software program would have blocked Internet searches on politically sensitive subjects and made computers more vulnerable to hackers. Companies persuaded the United States government to protest the Green Dam requirement because it violated free trade obligations under WTO rules. We need to see that kind of public-private partnership at work across the board on issues involving cyber-security and Internet freedom.

It's also very much in the interest of U.S. business to make such a partnership work. Brand integrity of U.S. entities is at stake when someone hacks into and alters or steals the intellectual property of U.S. companies such as Google. Melissa Hathaway, author of President Obama's recent cyber-space policy review, suggests that the government may need to retool our intelligence and diplomatic communities to protect U.S. intellectual property abroad.

Finally, and perhaps most troubling, is the way cyber-technology can be exploited to undermine our own security. Make no mistake: Not only are sophisticated and network-secure companies like Google vulnerable to attack from foreign countries, but the entire U.S. network faces assault on a daily basis. As recently noted by Deputy Defense Secretary Lynn, an adversarial nation could deploy hackers to take down U.S. financial systems, communications and infrastructure at a cost far below that of building a trillion-dollar fleet of jet fighters or an aircraft carrier.

China's alleged hacking of Google and subsequent reports that Google is partnering with the National Security Agency to analyze the attack raise some relevant questions for this committee: Does an unauthorized electronic intrusion constitute a violation of national sovereignty, equivalent to a physical trespass onto U.S. territory – and if so, what's the appropriate response?

We also need to consider the foreign policy implications of offensive U.S. capabilities. The United States has much to lose from a lawless cyberspace, where countries can attack each other at will and engage in a perennial low-intensity cyber conflict.

We look forward to hearing from our witnesses on how we can simultaneously promote Internet freedom and deprive repressive regimes of the tools of cyber-repression; and how we can promote the global diffusion of the Internet while also protecting ourselves from cyber-attack.

---

COMMITTEE ON FOREIGN AFFAIRS
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C. 20515

STATEMENT OF
THE HONORABLE ENI F.H. FALEOMAVAEGA
CHAIRMAN

before the
COMMITTEE ON FOREIGN AFFAIRS

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

MARCH 10, 2010

Mr. Chairman, the giant leaps in communications technology and cyberspace of recent decades have altered the way we live, the way we work and the way ideas and innovations spread.

The opportunities presented by massive new flows of information in economic, social, cultural and political terms cannot be underestimated. Yet, as with any radical technological change, a number of significant challenges have arisen as well. In cyberspace, these have taken the form of lost privacy, diminished security, threatened intellectual property, and sometimes, thoughtful deliberation of problems of local, national, and global import.

As we grapple with cyberspace policy, the Google case presents a compelling story. After all, the company is at the leading edge of technological change. Moreover, China – where the hackers were based – has increasingly become an object of fascination for the public and, unfortunately, a target for those seeking a country to demonize, whether for political or other purposes.

While the full story of this case has yet to be told, Google remains committed to China. On January 29, 2010, the company's chief executive officer, Eric Schmidt, said, "We love what China is doing as a country and its growth. We just don't like the censorship. We hope to apply some negotiation or pressure to make things better for the Chinese people."

In any case, Google's problems are only symptomatic of the larger issues at stake, ones truly global in scope. Mr. Chairman, thank you for calling this hearing. I hope it will be the first of many as the cyber commons continues to evolve and grow, and as we shape our cyber policies to benefit our own citizens and people all around the world.

**OPENING STATEMENT OF**
**THE HONORABLE RUSS CARNAHAN (MO-03)**
**COMMITTEE ON FOREIGN AFFAIRS**
**U.S. HOUSE OF REPRESENTATIVES**

**Hearing on**
***The Google Predicament:***
***Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade***
**Wednesday, March 10, 2010, 10:00 a.m.**
**2172 Rayburn House Office Building**

Chairman Berman and Ranking Member Ros-Lehtinen, thank you for holding this hearing regarding Google's efforts in China and U.S. cyber-security policy more broadly. I would also like to thank our witnesses from Google, the Center for Information Technology Policy, the Business Software Alliance, and the U.S.-China Economic and Security Review Commission.

As Chair of the Subcommittee on International Organizations, Human Rights, and Oversight, I'd first like to turn to the Universal Declaration of Human Rights, adopted in 1948 under the Truman Administration. Article 19 says, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

The United States has a rich, complex, and growing relationship with China. China's emergence in the global economy has lifted hundreds of millions of people out of poverty. China's growth can be mutually beneficial for the Chinese and American people, but it should not come at the expense of basic human rights. As Secretary Clinton said in her January 21 speech, "the internet has already been a source of tremendous progress in China.... But countries that restrict free access to information or violate the basic rights of internet users risk walling themselves off from the progress of the next century."

So what can be done? I'd like to praise voluntary private initiatives such as the Global Network Initiative, which includes organizations such as Google, Microsoft, Yahoo. The Global Network Initiative has developed a set of Principles on Freedom of Expression and Privacy and accompanying Implementation Guidelines. It is critical that there is clear and transparent enforcement mechanisms, so that corporations, academics, and non-governmental organizations can help hold each other accountable. These types of voluntary guidelines will be critical in protecting and promoting freedom of expression.

I'm also interested in how we can better use social media such as Twitter and Youtube to promote the free flow of information in Iran, North Korea, and other repressive regimes.

Thank you for holding this hearing today on such a critical and timely topic.

---

**The Honorable Gerald E. Connolly (VA-11)**

**HCFA Full Committee Hearing: The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade**
**Wednesday, March 10, 2010**
**10am**

Recent events, such as cyber attacks on at least twenty American companies that specialize in a variety of sectors, underscore the need for a comprehensive cybersecurity plan that can provide a framework to safeguard companies and individuals against cyber attacks, particularly attacks that originate from foreign soil. Representatives from internet search company Google have unequivocally stated that the recent attacks originated from China. It is even more troubling that internet security experts speculate that these attacks were not a series of isolated incidents, but part of a centrally organized attack. Whether or not these cyber attacks were part of a consolidated effort from a foreign power, the fact remains that the United States ought to have a centralized cyber security policy. Any such policy ought to take into account any potential affect on innovation, security, and human rights.

The wealth of information that one can harness from the internet is nearly boundless. This is especially useful for burgeoning democracy movements in countries such as Iran. The power of instantaneous updates through social networks can organize citizens into a cohesive, mass movement and inform those outside the country's borders of what transpires.

Though this development is positive, there are forces at work that undermine technological innovation. Intellectual property theft of software is all too common, and small scale theft of movies or software is no longer the biggest issue that U.S. companies face. The increasingly common "organizational end-use piracy" is a formidable threat to innovative companies. Additionally, countries like China have complex sets of rules and regulations governing software use. This puts American companies at a competitive disadvantage and may even reveal proprietary information. But American companies have not been passive. In 2008, Google, Yahoo, and Microsoft joined the Global Network Initiative, a code of conduct for free expression and privacy in the internet technology sector. This is a good step, as public-private partnerships are necessary to facilitate free expression.

It is unfortunate that the internet, an entity that is known for its abundance of information, has become a target of regimes that seek to limit information in the hopes of controlling their populations. A memorable example was Iran's cyber blockade of social networking sites in the aftermath of that country's fraudulent elections. Moreover, computer experts in China have hacked into the email accounts of prominent human rights activists. Hackers originating in China have even targeted Congressional Committees. But Iran and China are not the only offenders—at least thirteen countries have blocked YouTube, and at least seven countries have blocked blogging websites.

China's dismal human rights record only adds to the suspicion of that country's intentions with regard to intellectual property and free expression. Given the Google events and the Administration's new Cyberspace Policy Review, I could not think of a better time for this hearing. I look forward to the testimony of our witnesses.

---

**Statement of Congressman Gene Green**
**House Foreign Affairs Committee**
**"The Google Predicament: Transforming U.S. Cyber Space Policy to Advance Democracy, Security, and Trade"**
**March 10, 2010**

Mr. Chairman, thank you for holding this hearing today, and I would like to welcome our distinguished panelists.

The proliferation of the internet and other technologies has opened the door for global engagement, communication and commerce.

Unfortunately, these opportunities have also paved the way for increased security vulnerabilities and information and media restrictions.

On January 12, 2010 news sources reported that Google experienced an intrusion into its systems in mid-December.
Further investigation by Google discovered that third parties had routinely accessed the accounts of dozens of Chinese and foreign human rights advocates.

Following the attack, Google announced that it will no longer censor its search engine results.

Although China's government is among the most aggressive in censoring the information of its citizens, many other regimes have adopted these practices.

Freedom of information and democracy go hand in hand, and we must continue to ensure that the international community upholds these principles for all their citizens.

As we advocate for this freedom of information, we must also look at strengthening our internet vulnerabilities so that we do not put our national security at risk.

Thank you again, Mr. Chairman, for holding this hearing and I look forward to the testimony of our witnesses.

**Congresswoman Barbara Lee, of California**
**Questions for the Record**

**Committee on Foreign Affairs**
*"The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade"*

2172 Rayburn HOB
10:00 a.m.
March 10, 2010

Questions submitted to Nicole Wong, Esq., Vice President and Deputy General Counsel, Google, Inc.

***Domestic Surveillance/National Security***

**Q1:** As former victim of domestic surveillance under the Nixon Administration, I have serious concerns regarding the trajectory of the United States intelligence and national security framework.

I strongly opposed the Bush Administration's flagrant abuse of power under its warrantless wiretapping program, which undermined the American people's faith in government as well as American companies with regard to their privacy and security of their personal information.

These concerns remain and I wonder if the panel can provide some insight.

*How can we balance the potential applications and benefits of cyber technologies to our national security framework without compromising the individual liberties and constitutional rights of the American people?*

**Response was not available at the time of printing.**

***Consumer/Privacy Protections***

**Q1:** *With the proliferation of internet technologies and increasing electronic flow of personal information across all sectors, from financial services to healthcare, what steps can the government take, as well as the private sector, to protect individuals from foreign or domestic parties seeking to illegally access their sensitive information?*

**Response was not available at the time of printing.**

**Q2:** *What specific recourse do consumers currently have if a company fails to adequately protect their information?*

**Response was not available at the time of printing.**

***Cuba***

**Q1:** *The U.S. Chamber of Commerce has said quite plainly that our unilateral embargo of Cuba sequesters "the United States from its allies while denying U.S. companies access to markets in which third-country firms can do business easily."*

*Does Google or other internet technology providers currently operate or offer any services in Cuba?*

*If the United States were to improve relations with Cuba and liberalize our policies with regard to trade and commerce, do you believe American companies including Google would pursue opportunities in this market?*

**Response was not available at the time of printing.**

*Does your respective enterprise support liberalizing economic and trade relations between the United States and Cuba?*

**Response was not available at the time of printing.**

**Congresswoman Barbara Lee, of California**
**Questions for the Record**

**Committee on Foreign Affairs**
*"The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade"*

2172 Rayburn HOB
10:00 a.m.
March 10, 2010

Response from Ms. Rebecca MacKinnon, Visiting Fellow, Center for Information Technology Policy, Princeton University, Cofounder of Global Voices Online

***Domestic Surveillance/National Security***

**Q1:** As former victim of domestic surveillance under the Nixon Administration, I have serious concerns regarding the trajectory of the United States intelligence and national security framework.

I strongly opposed the Bush Administration's flagrant abuse of power under its warrantless wiretapping program, which undermined the American people's faith in government as well as American companies with regard to their privacy and security of their personal information.

These concerns remain and I wonder if the panel can provide some insight.

*How can we balance the potential applications and benefits of cyber technologies to our national security framework without compromising the individual liberties and constitutional rights of the American people?*

**Answer:**

Thanks very much for your concerns and your questions. My own parents were victims of domestic surveillance under Nixon and I share your concerns wholeheartedly. Our founding fathers engaged in heated debates about the best balance between freedom and security: total freedom leads to anarchy and insecurity while total security leads to a locked-down police state. The challenge of our time is to find the right balance between freedom and security in the digital age so that we can protect ourselves adequately from attack while at the same time prevent the forfeiture of our hard-won rights. We must be perpetually vigilant against abuses by those who hold power over us either politically or commercially. For this reason I believe that the PATRIOT Act should be reformed. Accountability and civil liberties safeguards surrounding government surveillance must be bolstered in order to protect against abuse. Congress should

revoke the FISA Amendments Act of 2008 which granted unacceptable levels of immunity to companies assisting in unaccountable and unconstitutional acts of government surveillance.

***Consumer/Privacy Protections***

**Q1:** *With the proliferation of internet technologies and increasing electronic flow of personal information across all sectors, from financial services to healthcare, what steps can the government take, as well as the private sector, to protect individuals from foreign or domestic parties seeking to illegally access their sensitive information?*

**Answer:**

If we were to eliminate the possibility of anonymity and privacy on the Internet, security would be easier, but that would also greatly reduce the possibility for dissent and whistle-blowing that are critical for a healthy democracy. I hope that Congress will resist the urge to lock down our digital infrastructure to the point that our rights to free expression and assembly will be squeezed to an unacceptable degree. While our banks, hospitals, and corporations are in an arms race with the criminals, beefing up the technical knowledge and skills of IT security departments around the country is the first step – in many cases security breaches have as much to do with the skill levels of personnel in the private sector as with government measures. Better education of the general public is also critical. Right now many attacks are enabled by uninformed behavior by members of the public and non-technical employees who have not been educated to recognize e-mail spoofs and phishing attacks, or who engage in unsafe Internet activities without understanding the extent to which they are exposing their home, school, or corporate networks. Basic computer education in elementary and secondary schools should include education on basic Internet security including how to use anti-virus and anti-spyware software, and how to detect Internet fraud, phishing, and spoofing. A savvy and alert population is the baseline requirement for a stable and secure society. Unfortunately in the digital realm Americans are not adequately savvy or alert.

**Q2:** *What specific recourse do consumers currently have if a company fails to adequately protect their information?*

**Answer:**

Right now, the recourse and protections are inadequate. Unlike a number of other Western democracies, the U.S. currently has no general privacy protection law or privacy oversight agency. While U.S. is a member of the Organization for Economic Cooperation and Development, it has not adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in any substantive way in either the public or private sector. Laws governing

private sector use of consumer data should require minimal retention of data necessary for the purpose of delivering the product or service in question. Companies should be required to make explicit to consumers what data is being maintained, in what manner, to what purpose, and with whom it will be shared. They should further be required to obtain an explicit "opt in" from consumers when substantive changes are made to privacy policies.

***Cuba***

**Q1:** *The U.S. Chamber of Commerce has said quite plainly that our unilateral embargo of Cuba sequesters "the United States from its allies while denying U.S. companies access to markets in which third-country firms can do business easily."*

*Does Google or other internet technology providers currently operate or offer any services in Cuba?*
*If the United States were to improve relations with Cuba and liberalize our policies with regard to trade and commerce, do you believe American companies including Google would pursue opportunities in this market?*

**Answer:**
I believe these questions are addressed to Google. But it is my understanding that under the revised Treasury Department rules, it is now legal for Google to make its free web services available to Cubans, but not paid services. I certainly hope that Google will find a way to pursue opportunities that can help Cubans participate in the global discourse taking place on the Internet – a substantial segment of which is being conducted in Spanish – once such opportunities become legal.

**Responses of Robert Holleyman**
**President and CEO**
**Business Software Alliance**
**To**
**Congresswoman Barbara Lee, of California**
**Questions for the Record**

**House Committee on Foreign Affairs**

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

March 10, 2010

**Domestic Surveillance/National Security**

**Q1:**

*How can we balance the potential applications and benefits of cyber technologies to our national security framework without compromising the individual liberties and constitutional rights of the American people?*

**A:** Congress, the Executive and the Courts must weigh a variety of considerations in establishing, applying and interpreting the rules regarding national intelligence and law enforcement access to electronic communications. The role of the technology industry is considerably narrower: they must obey the law. What is critical from an industry perspective is that those laws are clear.

**Consumer/Privacy Protections**

**Q1:**

*With the proliferation of internet technologies and increasing electronic flow of personal information across all sectors, from financial services to healthcare, what steps can the government take, as well as the private sector, to protect individuals from foreign or domestic parties seeking to illegally access their sensitive information?*

**A:** Protecting sensitive information requires a solid, risk-based approach. Organizations must assess the sensitivity of the information they hold, the threats and risk they face, and implement security measures that are effective and appropriate to their activities. BSA has consistently supported the inclusion of such common sense requirements in data security and breach legislation, such as in HR 2221, which was passed by the House of Representatives in December 2009.

**Q2:**

*What specific recourse do consumers currently have if a company fails to adequately protect their information?*

**A:** The FTC, which has been a very effective enforcer of federal consumer protection laws, has brought many cases against organizations that were either misrepresenting the protection they would afford to the consumer data that they held, or were failing to put in place data security measures to which a consumer was fairly entitled. FTC actions have resulted in large financial settlements with alleged infringers, sending a powerful signal to the marketplace that organizations that hold consumer data have an obligation to protect it through appropriate and effective risk-based measures.

**Cuba**

**Q1:**

*Does Google or other internet technology providers currently operate or offer any services in Cuba?*

**A:** I am aware of no information that any BSA member company does business overseas in violation of any US embargo.

**Q2:**

*If the United States were to improve relations with Cuba and liberalize our policies with regard to trade and commerce, do you believe American companies including Google would pursue opportunities in this market?*

**A:** I am certain that many of my member companies would consider pursuing opportunities in Cuba if US policy toward Cuba were to change. This is a matter that would be decided company by company, based on each company's individual assessment of the possible risks and benefits of doing business in that market, as well as other factors including Cuba's record with regard to human rights such as freedom of expression.

**Q3:**

*Mr. Holleyman and Ms. Wong, do your respective enterprises support liberalizing economic and trade relations between the United States and Cuba?*

**A:** The Business Software Alliance does not have a position on this matter.

**Congresswoman Barbara Lee, of California**
**Questions for the Record**

**Committee on Foreign Affairs**
*"The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade"*

Response from Larry M. Wortzel, Ph.D., Commissioner, U.S.-China Economic and Security Review Commission

***Domestic Surveillance/National Security***

**Q1:** As former victim of domestic surveillance under the Nixon Administration, I have serious concerns regarding the trajectory of the United States intelligence and national security framework.

I strongly opposed the Bush Administration's flagrant abuse of power under its warrantless wiretapping program, which undermined the American people's faith in government as well as American companies with regard to their privacy and security of their personal information.

These concerns remain and I wonder if the panel can provide some insight.

*How can we balance the potential applications and benefits of cyber technologies to our national security framework without compromising the individual liberties and constitutional rights of the American people?*

**Answer:**

I understand your concerns about preventing violations of individual liberties and protecting the constitutional rights of the American people. However, I do not share your views on the subject. As a career intelligence officer with experience in counterintelligence and monitoring foreign electronic communications, I can tell you that there is strong oversight from the inspectors general in the intelligence community to ensure operations are legal and a high degree of awareness of the need to protect civil liberties among all of the members of the intelligence community with whom I had contact. In addition, United States intelligence officers receive long periods of training and continuing education to ensure they are aware of and comply with law and executive branch policy on protecting civil liberties.

I believe that the reform of the intelligence community activities undertaken in the wake of revelations about the activities during the Nixon administration, and subsequent oversight, has been effective. Further, in my view the intelligence community oversight provided by Congress prevents similar abuses.

As you may see from some of my work at The Heritage Foundation, I strongly support the Patriot Act. You can find my arguments, along with those of my co-authors, in "What a Comprehensive Intelligence Bill Should Contain," at http://www.heritage.org/Research/Reports/2004/09/What-a-Comprehensive-Intelligence-Bill-Should-Contain. I also discuss some of these issues in the Heritage Foundation Memorandum "American's do not Need a New Domestic Spy Agency," which can be found at http://www.heritage.org/Research/Reports/2003/01/Americans-Do-Not-Need-a-New-Domestic-Spy-Agency.

On November 17, 2009, I testified in front of the Senate Judiciary Committee Subcommittee on Terrorism and Homeland Security about electronic surveillance, cyber threats and protecting the civil liberties of Americans. An abstract of relevant parts of that testimony follows:

> As a full disclosure, early in my career, I worked on National Security Agency (NSA) programs and continued to be associated with some of them throughout my military career. Therefore, I have to admit to some bias in favor of that agency. The NSA will likely be given the responsibility of also being the headquarters of the USCYBERCOM. My personal experience with NSA leads me to tell you that I have no reservations about that agency taking the lead in implementing U.S. cyber defenses. The NSA and its predecessor organizations have continuously—and successfully—handled technical operations for our government since World War I. The Agency has decades of institutional experience, and highly skilled personnel who can operate in the electronic and cyber realms. NSA personnel also have the crucial linguistic capabilities to support investigations of foreign intrusions. The NSA has international relationships with American friends and allies and a wide range of relationships across industry. It is therefore best qualified to head the government's efforts in the cyber realm. I also want to point out that as a counterintelligence special agent, a foreign intelligence collector and a signals intelligence collector I underwent days of training and continual re-instruction on the nuances of gathering critical intelligence while still protecting the privacy rights of American citizens. Our entire Intelligence Community gets such training.
>
> While few dispute that the NSA should direct the United States' offensive cyber operations, some cite privacy concerns over NSA involvement in securing government networks. My experience is that the NSA is extremely sensitive to intelligence oversight issues; their operators get a great deal of training and have privacy concerns drilled into their heads by leaders, inspectors general, oversight personnel, and training officers. I am very comfortable with the job that NSA does to ensure that its employees adhere to

laws limiting the collection of information on United States persons.

If privacy for American citizens is a concern, also think about institutional culture. Since the time of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the 1975 Church Committee), agencies of the U.S. Intelligence Community have come under strict oversight and revised their training and operations. All of the agencies of the Intelligence Community must by law seek investigative warrants under the Foreign Intelligence and Surveillance Act to intrude into the privacy of Americans. If I remember correctly my own training as a human intelligence collector and counterintelligence special agent, some of the agencies that formed DHS could (and still can) conduct intrusive, warrantless searches at our borders or customs searches with little probable cause other than the judgment of the agent. Our laws permit such searches for good reason under certain circumstances, but I would argue that the institutional culture in some agencies of DHS is very different than that in other law enforcement and intelligence agencies.

***Consumer/Privacy Protections***

**Q1:** *With the proliferation of internet technologies and increasing electronic flow of personal information across all sectors, from financial services to healthcare, what steps can the government take, as well as the private sector, to protect individuals from foreign or domestic parties seeking to illegally access their sensitive information?*

**Answer:**

This question falls outside the purview of legislative mandate under which the U.S.-China Economic and Security Review Commission operates. Therefore, as a body, the Commission has not worked on the issues addressed.

**Q2:** *What specific recourse do consumers currently have if a company fails to adequately protect their information?*

**Answer:**

This question falls outside the purview of legislative mandate under which the U.S.-China Economic and Security Review Commission operates. Therefore, as a body, the Commission has not worked on the issues addressed.

***Cuba***

**Q1:** *The U.S. Chamber of Commerce has said quite plainly that our unilateral embargo of Cuba sequesters "the United States from its allies while denying U.S. companies access to markets in which third-country firms can do business easily."*

*Does Google or other internet technology providers currently operate or offer any services in Cuba?*

**Answer:**

This question falls outside the purview of legislative mandate under which the U.S.-China Economic and Security Review Commission operates. Therefore, as a body, the Commission has not worked on the issues addressed.

*If the United States were to improve relations with Cuba and liberalize our policies with regard to trade and commerce, do you believe American companies including Google would pursue opportunities in this market?*

**Answer:**

This question falls outside the purview of legislative mandate under which the U.S.-China Economic and Security Review Commission operates. Therefore, as a body, the Commission has not worked on the issues addressed.

**Congresswoman Ileana Ros-Lehtinen**
**Question for the Record**
**China-Google Hearing**
**March 10, 2010**

Nicole Wong, Esq. Vice President and Deputy General Counsel:

1. I understand that Google has a policy that prohibits users from displaying its advertising alongside unlawful content, since it would be inappropriate for Google to profit off of users' illegal use. How is Google enforcing this policy?

**Response was not available at the time of printing.**

---

Mr. Joseph Crowley
Questions for the Record
The Google Predicament: Transforming
U.S. Cyberspace Policy to Advance Democracy, Security, and Trade
Wednesday, March 10, 2010

To Nicole Wong (with Google):

1) You have praised efforts by the United States to address censorship through trade tools, specifically in the context of the Korean Free Trade Agreement. Could you elaborate further on that point, in particular the types of things you'd like to see in terms of trade?

   **Response was not available at the time of printing.**

2) Can you let us know of some specific ways that you believe the Internet has been helpful toward opening new avenues to freedom of expression in China?

   **Response was not available at the time of printing.**

3) Could you elaborate further on how censorship may be considered a barrier to trade? There has been some suggestion of raising censorship at the WTO. Do you see this as a realistic rules-based option, if not now, then at some point down the road?

   **Response was not available at the time of printing.**

4) I am concerned about pirating and intellectual property, and one area in particular where I have some concerns is with musicians and artists being paid for their work. Could you elaborate on what Google is doing to ensure that artists and musicians' songs cannot be downloaded for free, both in terms of browsers and also applications? If a copyright owner notices some material or an application that contains unauthorized copyrighted material, how does Google deal with that

   **Response was not available at the time of printing.**

**Responses of Robert Holleyman**
**President and CEO**
**Business Software Alliance**
**To**
**Congressman Chris Smith, of New Jersey**
**Questions for the Record**

**House Committee on Foreign Affairs**

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

March 10, 2010

**Q1:**

*BSA seems to have engaged China vigorously on issues of intellectual property. How has it engaged the Chinese government on issues of human rights?*

**A:** BSA member companies each have their own approach to complying with the laws in the jurisdictions in which they operate. This is not a matter on which BSA member companies act collectively.

---

Representative Michael T. McCaul
March 10, 2010
Hearing on the Google Predicament

Questions submitted to Nicole Wong, Esq., Vice President and Deputy General Counsel, Google, Inc.

Questions:

1. I again would like to commend Google for your decision to no longer allow censorships of results on Google's Chinese search engine. At the time, you announced that you would begin to discuss with the Chinese government whether Google will be allowed to operate an unfiltered search engine, and stated that if these talks were unsuccessful, Google may shut down operations in China. What steps have you taken since this statement to facilitate these discussions with the Chinese government? If China continues to hold its ground on censorship, do you still plan to shut down your operations in China? Can you comment on the implications of leaving companies like China's indigenous search engine, Baidu, to dominate the market?

   **Response was not available at the time of printing.**

2. I echo your concerns about growing problems with cyber security. Just last month I led efforts to pass the Cybersecurity Enhancement Act. This critical piece of legislation is essential to securing our federal computer networks from outside threats and securing much of our nation's critical infrastructure. I want to thank Mr. Holleyman for personally commending our efforts. While we work to better secure our networks in the United States, how can we encourage China and other countries to prosecute those who threaten cyber security and violate intellectual property rights? What steps can be taken to put pressure on these countries?

   **Response was not available at the time of printing.**

3. Earlier this week, the U.S. Treasury Department amended their regulations, adding general licenses authorizing the exportation to Iran, Sudan, and Cuba of personal Internet-based communications services, such as instant messaging and chat. How do you think this will affect the ability of citizens in these countries to communicate more effectively with each other and the outside world? Do you expect the governments in these countries, especially Iran, to take measures to curtail any increase in access afforded to their people?

   **Response was not available at the time of printing.**

Representative Michael T. McCaul
March 10, 2010
Hearing on the Google Predicament

Response from Ms. Rebecca MacKinnon, Visiting Fellow, Center for Information Technology Policy, Princeton University, Cofounder of Global Voices Online

Questions:

1. I again would like to commend Google for your decision to no longer allow censorships of results on Google's Chinese search engine. At the time, you announced that you would begin to discuss with the Chinese government whether Google will be allowed to operate an unfiltered search engine, and stated that if these talks were unsuccessful, Google may shut down operations in China. What steps have you taken since this statement to facilitate these discussions with the Chinese government? If China continues to hold its ground on censorship, do you still plan to shut down your operations in China? Can you comment on the implications of leaving companies like China's indigenous search engine, Baidu, to dominate the market?

Answer:

This question is directed at Google only. I am not in a position to speak for Google. Also, since Google moved its Chinese search engine to Hong Kong last week, the question would appear to be moot.

2. I echo your concerns about growing problems with cyber security. Just last month I led efforts to pass the Cybersecurity Enhancement Act. This critical piece of legislation is essential to securing our federal computer networks from outside threats and securing much of our nation's critical infrastructure. I want to thank Mr. Holleyman for personally commending our efforts. While we work to better secure our networks in the United States, how can we encourage China and other countries to prosecute those who threaten cyber security and

violate intellectual property rights? What steps can be taken to put pressure on these countries?

Answer:

A big problem is that it is difficult to prove who carried out a cyber-attack, making it easy for governments to deny responsibility for attacks. The world lacks international agreements and frameworks through which governments might be held accountable for attacks originating from servers within their jurisdiction. Just as arms control treaties prevented disastrous escalation and unnecessary conflict in past decades, there is now an urgent need for a new set of cybersecurity treaties through which the obligations and responsibilities of governments, corporations, and other entities for maintaining the security and stability of the global Internet are clearly laid out.

3. Earlier this week, the U.S. Treasury Department amended their regulations, adding general licenses authorizing the exportation to Iran, Sudan, and Cuba of personal Internet-based communications services, such as instant messaging and chat. How do you think this will affect the ability of citizens in these countries to communicate more effectively with each other and the outside world? Do you expect the governments in these countries, especially Iran, to take measures to curtail any increase in access afforded to their people?

Answer:

This was a good first step. Right now, the amendment only covers free services and does not extend to people in Syria, Myanmar or North Korea, where activists remain shut out. Also, the latest changes do not cover any paid services such as website hosting or downloadable web development software. Iranian activists have recently pointed out to me that the inability to purchase consumer-grade equipment has also hindered their ability to communicate and organize.

Regarding measures by the Iranian government, I think it is fair to expect that this will continue to be a technology arms race between government and people. Unfortunately, the Iranian government can find ways to purchase

what they need from other countries, while individuals suffer the most from the embargo.

**Responses of Robert Holleyman**
**President and CEO**
**Business Software Alliance**
**To**
**Congressman Michael T. McCaul, of Texas**
**Questions for the Record**

**House Committee on Foreign Affairs**

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

March 10, 2010

**Q1:**

*I again would like to commend Google for your decision to no longer allow censorships of results on Google's Chinese search engine. At the time, you announced that you would begin to discuss with the Chinese government whether Google will be allowed to operate an unfiltered search engine, and stated that if these talks were unsuccessful, Google may shut down operations in China. What steps have you taken since this statement to facilitate these discussions with the Chinese government? If China continues to hold its ground on censorship, do you still plan to shut down your operations in China? Can you comment on the implications of leaving companies like China's indigenous search engine, Baidu, to dominate the market?*

**A:** This question is not directed to BSA.

**Q2:**

*I echo your concerns about growing problems with cyber security. Just last month I led efforts to pass the Cybersecurity Enhancement Act. This critical piece of legislation is essential to securing our federal computer networks from outside threats and securing much of our nation's critical infrastructure. I want to thank Mr. Holleyman for personally commending our efforts. While we work to better secure our networks in the United States, how can we encourage China and other countries to prosecute those who threaten cyber security and violate intellectual property rights? What steps can be taken to put pressure on these countries?*

**A:** BSA members believe that coordinated and continuous engagement of Chinese authorities by the US Government is necessary to secure tangible commitments about the prosecution of cybercriminals and IP infringers. This engagement must make these issues a priority. We believe it is in China's interest to crack down on these two problems, so that its own cyberspace is secure and its domestic intellectual property-based industry has the incentive to develop.

**Q3:**

*Earlier this week, the U.S. Treasury Department amended their regulations, adding general licenses authorizing the exportation to Iran, Sudan, and Cuba of personal Internet-based communications services, such as instant messaging and chat. How do you think this will affect the ability of citizens in these countries to communicate more effectively with each other and the outside world? Do you expect the governments in these countries, especially Iran, to take measures to curtail any increase in access afforded to their people?*

**A:** I do believe that this change in policy will have some positive impact on the ability of citizens in Iran, Sudan and Cuba to communicate. However, I am under no illusion that these governments won't take steps to curtail or control the use of these technologies. These are governments that seek to maintain tight control over the Internet within their borders, creating challenges for their citizens and for companies that seek to provide Internet-based communications.

Representative Michael T. McCaul
March 10, 2010
Hearing on the Google Predicament
Questions for the Record

Response from Larry M. Wortzel, Ph.D., Commissioner, U.S.-China Economic and Security Review Commission

1. I again would like to commend Google for your decision to no longer allow censorships of results on Google's Chinese search engine. At the time, you announced that you would begin to discuss with the Chinese government whether Google will be allowed to operate an unfiltered search engine, and stated that if these talks were unsuccessful, Google may shut down operations in China. What steps have you taken since this statement to facilitate these discussions with the Chinese government? If China continues to hold its ground on censorship, do you still plan to shut down your operations in China? Can you comment on the implications of leaving companies like China's indigenous search engine, Baidu, to dominate the market?

**Answer:**

This question falls outside the purview of legislative mandate under which the U.S.-China Economic and Security Review Commission operates. Therefore, as a body, the Commission has not worked on the issues addressed.

2. I echo your concerns about growing problems with cyber security. Just last month I led efforts to pass the Cybersecurity Enhancement Act. This critical piece of legislation is essential to securing our federal computer networks from outside threats and securing much of our nation's critical infrastructure. I want to thank Mr. Holleyman for personally commending our efforts. While we work to better secure our networks in the United States, how can we encourage China and other countries to prosecute those who threaten cyber security and violate intellectual property rights? What steps can be taken to put pressure on these countries?

**Answer:**

I would like to parse this question slightly so as to better address its components. The threat China poses to our nation's cyber security is different in many respects from the threat China poses by the theft of U.S. intellectual property. I will address each issue in turn.

First, however, please allow me to suggest that criminal prosecution is only one means to address these problems—and it may not be the most effective means. Certainly criminal law needs to be strengthened and broadened across international boundaries.

China is a sovereign nation, and though it does not have a separation of powers among parts of its government, its judicial system is resistant to outside pressure. Experience in trying to get China to prosecute more vigorously intellectual property violations has not been satisfactory. More important, a focus on punishing individuals diverts attention from China's government; it is likely that the government is directing keyboard activity. China and its Internet providers demonstrate an uncanny ability to control Internet traffic and the content available to Chinese people. It follows that properly motivated Chinese authorities could address the root of the problem—namely, the malicious cyber activity itself—if they so chose. This is better than reactively seeking justice, which in any case does not restore national security information or valuable American intellectual property.

**Cyber security:** To mitigate malicious cyber activity targeting U.S. government and industrial networks, we ought to employ a three-pronged strategy: robust defense, traps to catch malicious actors, good forensics, and when possible aggressive offense. Finally, we need tough diplomacy that is coordinated with allies. Recently both Germany and the UK have complained about malicious Chinese cyber activity.

First, to better protect ourselves and our information, we must recognize that firewalls are necessary but not sufficient. Government entities and firms must move toward a "defense in depth" strategy to safeguard each node, monitor every connection, and protect every user on our networks. We need to develop technologies to identify threats (thus enhance our "situational awareness") within our information systems. To do so, we must refine our ability to discern potentially harmful traffic within our networks.

We also need to regain the initiative in cyberspace by assembling, analyzing, and carefully exploiting intelligence we gain from attacks on our networks (and other information openly available on the Internet). And we need to share this information with trusted industry and private business partners. Our nation's high level of connectivity leaves us vulnerable, so any "active cyber response" we employ must be measured and carefully weighed against other options.

In addition, we need to use diplomacy to address cyber issues while developing the legal system to respond. The Internet is a public good, and we need to foster better working relationships with other countries to share the burden of enforcement activities. Moreover, the United States should outline a credible declaratory policy linking a kinetic response to certain types of aggressive cyber activity; this may help establish some much-needed boundaries in cyberspace. In addition, we should leverage domestic policies that have diplomatic implications. For example, we could couple malicious cyber activity—particularly that which targets critical infrastructure—to the responsible nations' intelligence collection priority ranking.

**Intellectual property:** Industry too must strengthen information security practices. But aggressive diplomacy and international alliances are the most effective means to combat the theft of intellectual property. Ultimately, we need to establish new channels to enforce intellectual property claims made against actors in other countries. The World Trade Organization (WTO) may be the best venue for this, and we should vigorously pursue WTO actions to counter China's disregard for intellectual property rights. This point became especially salient when Google announced earlier this year that the penetration of its networks in China targeted not only information about human rights activists, but also the company's valuable source code.

Stemming loses from online piracy and other less-sophisticated but more prevalent types of attacks may prove more challenging. However, the United States can and should champion a multinational organization that facilitates a process by which patent and copyright holders can complain to foreign Internet Service Providers (ISPs) that host protected content. We should also create incentives for these ISPs to remove pirated content of the basis of these tips. We should engage other stakeholders with an interest in the lawful use of the Internet. For example, the Internet Corporation for Assigned Names and Numbers (ICANN) could potentially impose penalties for noncompliance of intellectual property protections. Alternatively, agreements with—or legal mandates for—major telecommunications providers to step up enforcement could counter piracy.

3. Earlier this week, the U.S. Treasury Department amended their regulations, adding general licenses authorizing the exportation to Iran, Sudan, and Cuba of personal Internet-based communications services, such as instant messaging and chat. How do you think this will affect the ability of citizens in these countries to communicate more effectively with each other and the outside world? Do you expect the governments in these countries, especially Iran, to take measures to curtail any increase in access afforded to their people?

**Answer:**

This question falls outside the purview of legislative mandate under which the U.S.-China Economic and Security Review Commission operates. Therefore, as a body, the Commission has not worked on the issues addressed.

○