S. HRG. 110–643

GLOBAL INTERNET FREEDOM: CORPORATE RESPONSIBILITY AND THE RULE OF LAW

HEARING

BEFORE THE

SUBCOMMITTEE ON HUMAN RIGHTS AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

MAY 20, 2008

Serial No. J–110–93

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

45–688 PDF WASHINGTON : 2008

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

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts	ARLEN SPECTER, Pennsylvania
JOSEPH R. BIDEN, JR., Delaware	ORRIN G. HATCH, Utah
HERB KOHL, Wisconsin	CHARLES E. GRASSLEY, Iowa
DIANNE FEINSTEIN, California	JON KYL, Arizona
RUSSELL D. FEINGOLD, Wisconsin	JEFF SESSIONS, Alabama
CHARLES E. SCHUMER, New York	LINDSEY O. GRAHAM, South Carolina
RICHARD J. DURBIN, Illinois	JOHN CORNYN, Texas
BENJAMIN L. CARDIN, Maryland	SAM BROWNBACK, Kansas
SHELDON WHITEHOUSE, Rhode Island	TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
STEPHANIE A. MIDDLETON, *Republican Staff Director*
NICHOLAS A. ROSSI, *Republican Chief Counsel*

SUBCOMMITTEE ON HUMAN RIGHTS AND THE LAW

RICHARD J. DURBIN, Illinois, *Chairman*

EDWARD M. KENNEDY, Massachusetts	TOM COBURN, Oklahoma
JOSEPH R. BIDEN, JR., Delaware	JON KYL, Arizona
RUSSELL D. FEINGOLD, Wisconsin	LINDSEY O. GRAHAM, South Carolina
BENJAMIN L. CARDIN, Maryland	JOHN CORNYN, Texas
SHELDON WHITEHOUSE, Rhode Island	SAM BROWNBACK, Kansas

JOSEPH ZOGBY, *Chief Counsel*
BROOKE BACAK, *Republican Chief Counsel*

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Coburn, Hon. Tom, a U.S. Senator from the State of Oklahoma	4
prepared statement	90
Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois	1
prepared statement	95

WITNESSES

Chandler, Mark, Senior Vice President, General Counsel and Secretary, Cisco Systems, Inc., San Jose, California	12
Ganesan, Arvind, Director, Business and Human Rights Program, Human Rights Watch, Washington, D.C.	10
Samway, Michael, Vice President and General Counsel, Yahoo! Inc., Miami, Florida	8
Wong, Nicole, Deputy General Counsel, Google Inc., Mountain View, California	6
Zhou, Shiyu, Deputy Director, Global Internet Freedom Consortium, Bethesda, Maryland	15

QUESTIONS AND ANSWERS

Responses of Mark Chandler to questions submitted by Senators Durbin Coburn	36
Responses of Arvind Ganesan to questions submitted by Senator Coburn	47
Responses of Michael Samway to questions submitted by Senators Durbin and Coburn	50
Responses of Nicole Wong to questions submitted by Senators Durbin, Brownback and Coburn	63
Responses of Shiyu Zhou to questions submitted by Senator Coburn	81

SUBMISSIONS FOR THE RECORD

Amnesty International USA, New York, New York, statement	83
Chandler, Mark, Senior Vice President, General Counsel and Secretary, Cisco Systems, Inc., San Jose, California, statement	86
Computer & Communications Industry Association, Washington, D.C., statement	92
Ganesan, Arvind, Director, Business and Human Rights Program, Human Rights Watch, Washington, D.C., statement	98
Harris, Leslie, President/CEO, Center for Democracy & Technology, Washington, D.C., statement	107
New York Times, November 10, 2008, article	117
Palfrey, John G., Jr., Clinical Professor of Law & Executive Director, and Colin Maclay, Managing Director, Berkman Center for Internet & Society, Harvard Law School, Cambridge, Massachusetts, statement	119
Reporters Without Borders, Lucie Morillon, Director and Clothilde Le Coz, Internet Freedom Director, Washington, D.C., statement	128
Samway, Michael, Vice President and General Counsel, Yahoo! Inc., Miami, Florida, statement	138
Wong, Nicole, Deputy General Counsel, Google Inc., Mountain View, California, statement	141
World Organization for Human Rights USA, Washington, D.C., statement	152

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

Page

Zhou, Shiyu, Deputy Director, Global Internet Freedom Consortium, Bethesda, Maryland, statements 157

GLOBAL INTERNET FREEDOM: CORPORATE RESPONSIBILITY AND THE RULE OF LAW

TUESDAY, MAY 20, 2008

U.S. SENATE,
SUBCOMMITTEE ON HUMAN RIGHTS AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Subcommittee met, pursuant to notice, at 10:07 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Richard J. Durbin, Chairman of the Subcommittee, presiding.

Present: Senators Durbin, Cardin, Whitehouse, and Coburn.

OPENING STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR FROM THE STATE OF ILLINOIS

Chairman DURBIN. The Judiciary Committee's Subcommittee on Human Rights and the Law will come to order. I notice the witnesses are still standing, so I will ask at this point if they will please raise their right hand and repeat after me. Do you affirm that the testimony you are about to give before the Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Ms. WONG. I do.

Mr. SAMWAY. I do.

Mr. GANESAN. I do.

Mr. CHANDLER. I do.

Mr. ZHOU. I do.

Chairman DURBIN. Thank you. Let the record reflect that the witnesses have responded in the affirmative. Please be seated.

The subject of this hearing is "Global Internet Freedom: Corporate Responsibility and the Rule of Law." After a few opening remarks, I will recognize my colleague Senator Coburn, the Subcommittee's Ranking Member, for an opening statement, then turn to our witnesses.

I just might say that this morning I visited the Newseum for the first time, as part of a taping of a cable show for Illinois. It is a very impressive place to visit. And I could not think of a more timely visit in light of this hearing. They have on display there a map of the world and a grading system as to which countries in the world are most open and free when it comes to speech and press and the basic freedoms which we have enshrined in our Constitution. And, sadly, too many are found deficient—even our own country, in many respects, deficient in aspiring to the values that are part of our credo as Americans. This was a perfect visit in terms of what we are doing today in talking about the question of Inter-

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

net freedom and the responsibility of American companies around the world.

There is a tendency to view human rights as just a foreign policy issue, but in this Subcommittee we have learned that is an inaccurate perception. Our world is growing smaller every day, a process accelerated by the Internet revolution. We have seen that human rights violations in other countries can affect us. To take one example, this Subcommittee has discovered that over 1,000 war criminals from other countries have found safe haven in the United States of America. On the other side, the actions of the U.S. Government and U.S. companies affect human rights in other countries.

In future hearings, we are going to explore the impact of corporate America on other fundamental human rights, but today we are going to focus specifically on the role of U.S. technology companies in Internet freedom around the world.

In 1791, the First Amendment to the Constitution was ratified, enshrining freedom of speech as the first fundamental right of all Americans. The First Amendment became an inspiration not only to Americans but to everyone around the world and inspired many to throw off the yoke of oppression.

The year 2008 is the 60th anniversary of the Universal Declaration of Human Rights. After World War II, under Eleanor Roosevelt's leadership, the United States spearheaded the ratification of the Universal Declaration, which recognized freedom of expression as a fundamental right of all people. The advent of the Internet has allowed billions of people to exercise this right more fully.

But the Internet is not free for everyone. Contrary to early predictions that the Internet could not be controlled, many countries censor the Internet and jail online dissidents. In Egypt, blogger Kareem Amer is serving a 4-year prison term for entries on his blog relating to Islam and President Hosni Mubarak. Now, just last month, 27-year-old Esra Abdel-Fattah was arrested after forming a group online to protest the high price of food in Egypt. She was released only in return for her promise to give up Internet activism.

In Cuba, citizens can be jailed for using the Internet for counterrevolutionary purposes. Cuban telecommunications Minister Ramiro Valdes said on February 27, 2007, that the Internet was a "tool for global extermination."

In Burma last fall, the military junta imposed a blackout on the Internet when images of Buddhist monks protesting the military's rule started appearing online.

And in China, dozens of bloggers have been jailed, including Hu Jia, who was recently sentenced to 3½ years in prison based in part on online essays he wrote criticizing the Chinese Government's human rights record. Three and a half years in prison simply for exercising his freedom of expression.

Over 30,000 Internet police monitor the Web in China, and the so-called Great Firewall of China prevents Chinese citizens from receiving accurate information about China's human rights record in Tibet and Darfur, among other subjects. The so-called Internet cops that are pictured here, these little cartoonish figures, pop up

periodically to remind users in China that their Internet usage is being monitored by the government.

In today's hearing, we will examine the role that American companies play in Internet censorship. At the outset, let me acknowledge the obvious: This is not a black- and-white issue, and it is not an easy issue. U.S. technology companies face difficult challenges when dealing with repressive governments, but these companies also have a moral obligation to protect freedom of expression.

You will see in the opening statements of virtually every witness here a statement stating that their companies, their corporate philosophies, are in favor of freedom of expression. I think that is good and right, but it really creates a standard for them and for us. And there is no question that some have fallen short of the mark on more than one occasion. In fact, perhaps it is time for Congress to consider converting this moral obligation into a legal obligation.

Human rights groups have accused Cisco of providing network equipment that forms the backbone of the Great Firewall of China and is used by other repressive countries to censor Internet and monitor users. I want to note that last week the Subcommittee received some troubling information about Cisco's activities in China, which has been reported in the press, and I have had a meeting with Cisco, Mr. Chandler and others, to discuss it. This information has been shared with them and will be discussed further today.

Software produced by American companies such as Fortinet and Secure Computing has reportedly been used to censor the Internet in Burma and Iran, respectively. Google received significant public criticism when it decided to launch Google.cn, a China-specific search site that removes results to conform with China's censorship policies. We will show you some illustrations later in the hearing. And Microsoft removes the blogs of Internet activists from their blogging service in response to requests from repressive governments.

Not all the news is negative. Around the world, Internet activists are breaking down the walls of censorship. In Cuba, for example, students use flash drives, digital cameras, and clandestine Internet connections to post blog entries and download information. Yoani Sanchez, a Cuban blogger, poses as a tourist at Internet cafes to make posts on her blog. She was recently named one of Time Magazine's Most Influential People of 2008. Activists like Dr. Shiyu Zhou have developed technology that allows users to break through firewalls and avoid censorship.

Three of our witnesses—Yahoo!, Google, and Human Rights Watch—have been working for almost 2 years on developing a voluntary code of conduct for Internet companies that do business in repressive countries. I look forward to hearing about the status of this long-awaited initiative, and I challenge all here who are interested in the subject no longer to tolerate the delay in reaching this agreement.

As access to Internet continues to spread and change the way we inform and express ourselves, our Government and American companies will be challenged to promote free speech and not to facilitate repression. With our collective efforts, perhaps someday the Internet can fulfill its promise of empowering all people to exercise their right to seek information and express their opinions freely.

[The prepared statement of Senator Durbin appears as a submission for the record.]

I want to recognize Senator Coburn for an opening statement.

STATEMENT OF HON. TOM COBURN, A U.S. SENATOR FROM THE STATE OF OKLAHOMA

Senator COBURN. Thank you, Senator Durbin. Again, another compelling hearing for this Subcommittee on Human Rights and the Law.

Senator Durbin and his staff are to be commended for their dedication of the issues of such heavy import. This relatively new Subcommittee has already proven to be quite a force, introducing bipartisan legislation to address genocide, human trafficking, and child soldiers. These bills are already well on their way to bringing justice to victims of the most egregious human rights abuses.

The Genocide Accountability Act has already been signed into law. My congratulations. The Child Soldiers Accountability Act passed the Senate by unanimous consent. And the Trafficking in Persons Accountability Act awaits consideration by the full Senate after receiving unanimous approval from the Senate Judiciary Committee.

This kind of progress is unusual in today's partisan atmosphere, but Senator Durbin and his staff have ensured success by reaching across the aisle to work together to tackle very complex and critical issues for freedom throughout the world. Under his leadership, we have approached every issue objectively, studying issues closely and talking to experts at both hearings and behind the scenes. In doing so, we have developed reasonable proposals to close gaps in current law that have inadvertently allowed the United States to serve as a safe haven for human rights perpetrators.

Today, we address the issue of Internet freedom. Nearly 1.5 billion people now use the Internet, 220 million of which reside in China. This number has more than doubled since early 2006 when the House of Representatives first held a hearing on this issue. The growth is explosive and, amazingly, China now has the largest Internet population in the world. The introduction and widespread use of this technology in countries like China is one of the most exciting developments of our day. Information is power. That information can become freedom, and the more that Chinese citizens have access to that information, the more open their society will inevitably be.

Of course, nobody understands the power of the Internet better than the governments who seek to repress their societies. I have already mentioned China, but that country is not the only government with such pernicious censorship. According to Reporters Without Borders, at least 62 cyber dissidents are currently imprisoned worldwide, with more than 2,600 websites, blogs, or discussion forums which were closed and made inaccessible in 2007 alone. The group has identified countries where Internet freedoms are restricted, which are China, Cuba, North Korea, Belarus, Burma, Egypt, Ethiopia, Iran, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, Vietnam, and Zimbabwe. It named 11 additional countries as "countries under watch." It is my hope that

today's hearing will shed light on how pervasive Internet censorship has become around the world.

This is not the first time Congress has addressed the issue of Internet freedom. The House of Representatives, led by Congressman Chris Smith and the late Congressman Tom Lantos, held two recent hearings and have thereby created a thorough record for our benefit. I would like to thank my colleagues for their dedication to the issue and the detailed groundwork that they have already laid.

The House hearings explored and established the factual record surrounding the relatively short history of American companies that have provided Internet service in countries where censorship is required by law. Those hearings examined in detail the steps and missteps of the companies as they began doing business in unfamiliar territory.

Mr. Chairman, it is my hope today that we will tackle the challenge of discussing possible solutions for the problems that face these companies. While understanding that the past is an important aspect of shaping solutions for the future, it is my hope that we can avoid relitigating the same issues that have already been discussed at length. Our panel of witnesses, which includes the industry experts and human rights advocates, should be able to explain the progress that has been made since the last hearing on this issue and answer questions that will help us better understanding the challenge of preserving Internet freedom around the world.

While the focus on this hearing is worldwide, it is also my hope that while the eyes of the world are on China in response to the massive earthquake and also there is some anticipation of the Summer Olympics, China's eyes are also on us as we criticize government censorship of the Internet and call for more freedom for their citizens. I view this time as an opportunity to show the people of China what freedom looks like and also to let the Chinese Government know that its actions have not gone unnoticed. This is just another opportunity to lead by example, which is what I hope American Internet companies doing business in places like China will also choose to do. Their presence in these places is important, and it is crucial that they operate on the side of those seeking freedom rather than oppression.

[The prepared statement of Senator Coburn appears as a submission for the record.]

I thank the Chairman, and I look forward to the witnesses' testimony.

Chairman DURBIN. Thank you, Senator Coburn. And I want to just add I appreciate the kind remarks at the outset, and none of this would have happened had we not been able to do it on a bipartisan basis. We have a very good positive, working relationship, and I know that that is going to continue.

And let me also acknowledge, as Senator Coburn has, the fine work that was done by the late Congressman Tom Lantos, a friend of many of us, who really led on this issue, and Chris Smith, who, again, made it a bipartisan effort in the House and continues to have an abiding interest in progress on this issue. We will work with our House colleagues on any legislation that we develop.

The record will reflect that we have sworn in the witnesses. Our first witness is Nicole Wong, Deputy General Counsel at Google. Ms. Wong is co-editor of "Electronic Media and Privacy Law Handbook." She was one of the founders and first editors-in-chief of the Asian Law Journal. In 2006, Ms. Wong was named one of the Best Lawyers under 40 by the National Asian-Pacific American Bar Association. She received her law degree and master's degree in journalism from the University of California at Berkeley.

Thank you for coming today. Your entire statement will be made part of the record, if you would like to summarize it at this point. After all the witnesses have spoken, we will ask questions.

STATEMENT OF NICOLE WONG, DEPUTY GENERAL COUNSEL, GOOGLE INC., MOUNTAIN VIEW, CALIFORNIA

Ms. WONG. Chairman Durbin, Ranking Member Coburn, members of the Subcommittee, thank you for inviting me to discuss with you the issue of Internet freedom. My name is Nicole Wong, and I am Google's Deputy General Counsel. In that role, I am responsible for helping to address limits on free speech that Google faces around the world.

Google's commitment to freedom of expression is at the core of everything we do. Our company's mission is to organize the world's information and make it universally accessible and useful. We provide Internet users with products that let them quickly and easily share, receive, and organize digital information. In theory, any person can use our free products that enable individual expression and information access.

However, freedom of expression on the Internet is not embraced universally. For example, since 2007, our YouTube video-sharing site has been blocked in at least 11 countries. In the last couple of years, we have received reports that our Blogger and Blog*Spot sites are being blocked in at least seven countries. And our social networking site, orkut, has been blocked recently in three countries.

With that in mind, I would like to make two main points in my testimony this morning. First, Google enables freedom of expression on a global platform, even as we deal with government efforts around the world to limit free expression. Second, governments around the world can and must do more to reduce Internet censorship.

Let me begin with an example of how our products are used as tools for free expression in countries that have attempted, and in some cases succeeded, in restricting speech in other media.

When the military government of Burma cracked down on protests by tens of thousands of Buddhist monks in the fall of 2007, it tried to do so outside of the public eye. During the protests, foreign journalists were kicked out of the country, national media was shut down, and Internet and cell phone services were disrupted within Burma in an effort to prevent information leaking out about the extent of the violence. Nevertheless, tools like Blogger and YouTube were used by citizen journalists to share videos of the protests and information about the extent of the blackout, enabling the rest of the world to witness the human rights abuses taking place within that country.

Because our technologies and services enable every person with an Internet connection to speak to a worldwide audience and, conversely, to read the stories and see the images posted beyond their national borders, Google has become a regular focus of governmental efforts to limit individual expression.

Just to fill out this picture, let me give you two examples. Over the past year in Turkey, the courts have blocked the entire YouTube site multiple times, for several days each, because of videos deemed insulting to Mustafa Kemal Ataturk, the founding father of modern Turkey, who has now been dead for 70 years, and other videos deemed by the Turkish Government to be threatening to their state, such as videos promoting an independent Kurdistan. Under Turkish law, these types of content are crimes. While we have been engaged with Turkish officials for many months, it has been difficult to even know which videos have been the source of complaint in order to address or challenge those bans.

Another example: In China in October 2007, at a time when the Dalai Lama was awarded the Congressional Gold Medal and the Communist Party Congress convened in Beijing, YouTube was blocked throughout China. While we were not informed of the exact cause of this suppression of speech and we did not ourselves remove any videos, access to the site in China was reinstated only following the conclusion of the Party Congress.

These are just two examples. Since the start of 2007, by our count Google services have been blocked, in whole or in part, in over 24 countries. As governments censor content online, we recognize that Internet companies have a shared responsibility to protect these important speech platforms and the people who use them as we deploy our services around the world.

Every day Google works to advance human rights through a variety of initiatives. As a start, we work hard to maximize the information available to users in every country where we offer our services. To the extent we are required to remove information from our search engine, for example, we make efforts to tell our users by placing a notice on the Search Results page. In China, we believe we are the least filtered, most transparent search engine available.

Google has also taken a leading role in working with companies and human rights groups to produce a set of principles on how companies respond to government policies that threaten speech and privacy online. We are also working with human rights bloggers and other groups to help them use our products to promote free speech online and to develop technology designed to defeat Internet censorship.

So let me now turn to my second point. We believe it is vital for the U.S. Government to do more to make Internet censorship a central element of our bilateral and multilateral agendas.

Mr. Chairman, the testimony I submitted to the Committee today includes detailed recommendations building on existing human rights mechanisms to reinvigorate the international community's commitment to free expression. There are two in particular I would call to the Committee's attention.

First, we have become convinced that a single company can only do so much to fight censorship regimes around the world, and to meet the challenges in this area. We recommend increased promi-

nence, authority, and funding be given to the State Department and the USTR. We continue to urge governments to recognize that information restrictions on the Internet have a trade dimension.

The bottom line is that much, much more can be done by the U.S., and at the international level by countries that respect free expression online, to ensure that individuals, companies, and others can use the Internet as the free and open platform it was designed to be.

I would like to conclude by thanking the Subcommittee for helping to highlight the importance of the Internet to free expression. It is only with the attention and involvement of leaders like yourselves that we can make real progress in the effort to combat censorship throughout the world.

Thank you.

[The prepared statement of Ms. Wong appears as a submission for the record.]

Chairman DURBIN. Thank you, Ms. Wong.

Our second witness is Michael Samway. He is the Vice President and Deputy General Counsel at Yahoo! Mr. Samway leads Yahoo!'s Business and Human Rights Program. He is also on the board of Yahoo!'s Human Rights Fund. Mr. Samway earned his B.S. and M.S. from the highly respected Georgetown University School of Foreign Service, was a Fulbright Scholar in Chile, and received a JD/LLM in International and Comparative Law from Duke Law School.

Mr. Samway, thank you for joining us. Please proceed.

STATEMENT OF MICHAEL SAMWAY, VICE PRESIDENT AND GENERAL COUNSEL, YAHOO! INC., MIAMI, FLORIDA

Mr. SAMWAY. Chairman Durbin, Ranking Member Coburn, members of the Subcommittee, my name is Michael Samway, and I am Vice President and Deputy General Counsel at Yahoo! I also lead Yahoo!'s global human rights efforts. I appreciate the opportunity to testify before you today.

At Yahoo!, we are deeply committed to human rights and to being a leader among technology companies in this area. Our company was founded on the principle that promoting access to information can fundamentally improve people's lives and enhance their relationship with the world around them. In the period since Yahoo!'s creation in 1994, the power and ubiquity of the Internet has exceeded even our most far-reaching expectations.

The Internet has dramatically changed the way people obtain information, communicate with each other, engage in civic discourse, conduct business, and more. Even in countries that restrict people's ability to communicate with one another or access information, people are still finding meaningful ways to engage online. Over the last week alone, we have seen just how important new communications technologies can be in places like China. Internet and cell phone resources have proven invaluable as government authorities and individuals contend with the aftermath of a devastating and enormously tragic earthquake in the Sichuan province.

With the goal of bringing Yahoo!'s technological tools to people around the world, we embarked on a mission to expand our business globally in the late 1990's. As one of the first Internet compa-

nies to explore the Chinese market, we launched a service with the belief that providing the people of China with innovative tools to communicate, learn, and even publish their own views was one effective means to improve their way of life.

We were joined in this strategy of engagement by many in Congress and in both Democratic and Republican administrations alike. With the sporadic pace of political progress in China as well as the need for companies there to adhere to local laws, we have also learned that expanding into emerging markets presents complex challenges that sometimes test even the important benefits of engagement itself.

While Yahoo! has not owned or had day-to-day control over Yahoo! China since 2005, we continue to be concerned about the challenges we faced in that market and will certainly face in other markets in the years to come.

Skeptics have questioned whether American Internet companies should engage in these countries at all. Yahoo! shares these concerns, and we have confronted these same questions about engagement in challenging markets. Yet we continue to believe in the Internet's transformative power and, on balance, its constructive role in transmitting information to, from, and within these countries. And we are committed to doing our part through supporting individual and collective action.

Governments, because of their enormous leverage, have a vital role to play. To that end, we have asked the U.S. Government to use its leverage—through trade relationships, bilateral and multilateral forums, and other diplomatic means—to create a global environment where Internet freedom is a priority and where people are no longer imprisoned for expressing their views online.

Our CEO, Jerry Yang, has met personally with State Department officials and earlier this year wrote a letter to Secretary Rice urging the State Department to redouble its efforts to secure the release of imprisoned Chinese dissidents. Secretary Rice raised this issue with senior Chinese officials, and since then we have seen Members of Congress echo this call for U.S. diplomatic leadership. We hope these efforts will both intensify and bear fruit.

We are also taking steps on our own. Jerry Yang announced the Yahoo! Human Rights Fund in November 2007, as part of a broader effort to address human rights challenges in China and around the world. We have partnered with noted dissident and human rights activist Harry Wu, who is here with us today, and the Laogai Research Foundation to establish this fund.

The Yahoo! Human Rights Fund will provide humanitarian and legal support to political dissidents who have been imprisoned for expressing their views online, as well as assistance for their families. A portion of the fund will also be used to support the Laogai Research Foundation's educational work to advance human rights.

In order to fuse our global business with responsible decision-making on human rights issues, we have also established the Yahoo! Business and Human Rights Program. A key pillar of this program is a formal assessment of the potential human rights impact of business plans we develop for new markets. This assessment examines the human rights landscape in a country, evaluates potential challenges to free expression and privacy, and offers stra-

tegic approaches to protect the rights of our users through legal and operational structures, among other methods. Yahoo! then tailors its entry into the new market to minimize risks to human rights.

Because it is so difficult for just one company to create systemic change, Yahoo! has also been a committed participant in a broad-based global human rights dialog. We are working with industry partners, academics, human rights groups, and socially responsible investors to develop a code of conduct that will guide technology companies operating in challenging markets. At Yahoo!, we are eager to make this global code a reality in the near future.

As an industry pioneer, Yahoo! is proud to have explored new ideas and markets, helping drive the transformative power of the Internet. Just like others who have gone first, Yahoo! has learned tough lessons about the challenges of doing business in nations with governments unlike our own. Yahoo! is working intensively and at the most senior levels in the company to set the highest standards for decisionmaking around human rights. The initiatives we pursue at Yahoo! are intended to protect the rights of our users, improve their lives, and make the extraordinary tools of the Internet safely and openly available to people around the world.

I appreciate the opportunity to tell you about these efforts to date and about our plans to continue to pursue a global leadership role in the field of human rights. I look forward to answering your questions.

Thank you.

[The prepared statement of Mr. Samway appears as a submission for the record.]

Chairman DURBIN. Thanks, Mr. Samway.

Our next witness is Arvind Ganesan, Director of the Business and Human Rights Program at Human Rights Watch. He has published three books and numerous articles on business and human rights. In 2006, he was the editor of the Human Rights Watch report "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship."

Thank you for being here. Please proceed.

STATEMENT OF ARVIND GANESAN, DIRECTOR, BUSINESS AND HUMAN RIGHTS PROGRAM, HUMAN RIGHTS WATCH, WASHINGTON, D.C.

Mr. GANESAN. Mr. Chairman, thank you for the opportunity to speak today, and thank you for your leadership on this issue. I would also like to thank members of the Subcommittee and, in particular, Senator Coburn. As somebody who is from Oklahoma, I have to say that my parents are thrilled about the prospect of me testifying in front of one of their Senators today.

Human Rights Watch believes that the Internet is a transformative force that can help open closed societies and provide the near instantaneous flow of information to inform the public, mobilize for change, and ultimately hold institutions accountable. However, today there is a real danger of a Virtual Curtain dividing the Internet, much as the Iron Curtain did during the cold war.

I would like to briefly address three issues in relation to global Internet freedom: the actions by some repressive governments to

restrict the flow of information and to punish individuals using the Internet; the ongoing efforts by industry to develop self-regulation to ensure that leading companies do not become complicit in abuses; and, finally, the prospects for government-led change.

In 2006, the human rights problems related to the Internet in China came to light. Yahoo! had provided user information to Chinese authorities that led to the imprisonment of online activists, and U.S. companies, including Google, Microsoft, and Yahoo!, censor their search engines in China. This is in anticipation of what Chinese censors expect and in addition to what the Chinese Government's firewall prohibits.

But China is not the only government that actively tries to suppress its critics in the virtual world. Others have intimidated or silenced activists on the Internet by controlling both providers and users.

The Russian Government is trying to replicate the Chinese firewall. It is promulgating a decree to spy on users, and it is also prosecuting an individual for posting a blog with an offensive suggestion that was ultimately critical of police corruption. And in January 2007, leading companies, including Yahoo!, Microsoft, and Google, along with human rights organizations, socially responsible investors, and academics, started a process to develop a voluntary code of conduct. The code was to contain a compliance mechanism to try to curtail censorship and protect user information.

Initially, we had hoped that the process could help stop companies from censoring and ensure that they protect cyber dissidents. But almost 18 months later, there is no system in place. We are still negotiating. In the meantime, Internet users are no safer and censorship continues.

Not every company is in the same place, nor is it fair to say companies do not care about human rights. And we have heard several examples of those approaches today. Those are laudable efforts, but they do not address steps companies should take to ensure that their operations do not contribute to abuses.

Without disclosing the details of discussions within the initiative, I can say that a fundamental problem is that some companies continue to be very resistant to the idea of independent monitoring. In particular, they are resistant to a system that would allow for an independent third party to assess: one, whether or not companies have put policies into place to reduce censorship and protect users; two, that those polices are diligently implemented; and, three, that their implementation is actually effective in curtailing these human rights problems. Unfortunately, the preferred option for some companies is a system in which they will decide who the monitors are, what they will see, and will implement those standards at a pace convenient to them.

In other words, companies will express support for human rights but also ask the public to basically trust them to do the right thing.

Sadly, it is difficult to point to any company within the voluntary initiative that has robust human rights policies and procedures in place more than 2 years after the problems in China were disclosed. Google, for example, has actively resisted such efforts. On May 8th, Google's board voted down two shareholder proposals. One called on the company to implement policies and procedures

to protect human rights, and the other called for a board committee on human rights. Sergey Brin, the company's co-founder, abstained from the vote because he felt that these proposals were not the appropriate way to approach the issue. Instead, he suggested a company discussion might be useful.

Google's resistant stance and the lack of consensus on voluntary standards raise a fundamental question: What is holding up these companies from implementing an effective means to protect user privacy and to curtail censorship?

My final point is on government. Legislation is an essential complement to a voluntary effort, and there is a promising bill in the House. A voluntary initiative will not apply to companies which do not join it, and it is difficult to see how it will be implemented under repressive governments who are very good at dividing and pressuring companies. Legislation would make it more difficult for repressive governments to force companies into becoming complicit in human rights abuses, and it might also encourage a more assertive U.S. foreign policy on these issues.

A useful model for this approach is the Foreign Corrupt Practices Act. That act mandates that companies will face penalties if they do not put adequate systems in place to prevent bribery, and it contains penalties if they actually engage in corruption. A similar approach could work quite well in regards to the Internet and would easily complement a voluntary initiative since it would require a company to put systems into place to prevent abuses and would hold them accountable if abuses occurred. Unfortunately, the companies are apparently resistant to legislation, much like they are resistant to effective voluntary measures.

Last weekend, news reports began to circulate about an Indian man who reportedly is facing charges for making critical and possibly vulgar comments about Sonia Gandhi online. He was reportedly identified with the help of Google because he was using their social networking site in India. We should not have to wait for another arrest to see progress from companies.

Thank you again, and I look forward to your questions.

[The prepared statement of Mr. Ganesan appears as a submission for the record.]

Chairman DURBIN. Thank you, Mr. Ganesan.

Our next witness is Mark Chandler, Senior Vice President, General Counsel, and Secretary of Cisco Systems. He has been with Cisco since 1996. He was previously General Counsel at StrataCom and Vice President and General Counsel of Maxtor Corporation. He is a member of several boards, including the Board of Visitors at Stanford Law, and the Advisory Council of the Woodrow Wilson International Center for Scholars in Washington. Mr. Chandler received his bachelor's degree from Harvard and his J.D. from Stanford Law School.

Mr. Chandler, thank you for joining us and please proceed.

STATEMENT OF MARK CHANDLER, SENIOR VICE PRESIDENT, GENERAL COUNSEL, AND SECRETARY, CISCO SYSTEMS, INC., SAN JOSE, CALIFORNIA

Mr. CHANDLER. Mr. Chairman, Ranking Member Coburn, my name is Mark Chandler. I am Senior Vice President and the Gen-

eral Counsel of Cisco. Thank you for the opportunity to appear before you today.

My company was founded 24 years ago by two Stanford graduate students. Today we have 65,000 employees around the world, more than 40,000 in the United States, including over 80 percent of our engineering. We are proud of the fact that we have added over 8,000 jobs in the United States in the last 2 years in difficult economic times.

I testified 2 years ago before Congressman Smith's Subcommittee on the topic of global Internet freedom. As a company that supports free expression and open communication, we recognize the importance of driving policies to enable people the world over to benefit from the freedom and empowerment that the Internet can offer. I want to reiterate five key points from that testimony 2 years ago.

First, Cisco sells the same products globally, built to global standards, thereby enhancing the free flow of information.

Second, Cisco's routers and switches include basic features that are essential to fundamental operation of the Internet by blocking hackers from interrupting services. protecting networks from viruses.

Third, those same features without which the Internet could not function effectively can, unfortunately, be used by network administrators for political and other purposes.

Fourth, in this regard, Cisco does not customize or develop specialized or unique filtering capabilities in order to enable different regimes to block access to information.

And, fifth, Cisco is not a service or content provider, nor are we a network manager who can determine how those features are used. These points were through 2 years ago, and they remain true today.

I do want to directly address the Cisco internal presentation that was provided to the Committee last week, which was prepared by a Chinese engineer inside Cisco in 2002, designed to inform Cisco employees in China about the history and operation of China's public safety organizations. I have the utmost respect for those like Professor Zhou who commit their lives and resources to the cause of free expression. And I am also grateful to him and to Ambassador Palmer and Michael Horowitz of the Hudson Institute for providing the presentation to us so we could translate it and review it in advance of today's hearing.

We were disappointed to find that the Cisco internal presentation included a Chinese Government official statement regarding combat and hostile elements, including religious organizations. We regret the engineer included that quote in the presentation, even by way of explaining the Chinese Government's goals, and we disavow the implication that this reflects in any way Cisco's views or objectives.

The nature of that presentation has not been accurately described, however. The document consisted of 90 PowerPoint slides reviewing various Government projects, including no fewer than 12 pages on the Beijing traffic management bureau and firefighting brigades. The presentation described products of various other companies, including China's Ra Wei, and U.S. companies, such as Lucent, Harris, and Motorola, in providing equipment to the Min-

istry of Public Security. It also described in detail the role that Cisco's standard networking products could play in facilitating communication. In no case—and I repeat, no case—did the document propose any Cisco products be provided to facilitate political goals of the government, and no reference was made to an application of our products to goals of censorship or monitoring.

We do not know how the Chinese Government implemented filtering or censorship beyond the basic intrusion protection and site filtering that all Internet routing products contain, such as used by libraries to block pornography.

For instance, Cisco does not provide the interception capabilities that comply with the CALEA statute in the U.S. We believe the mediation devices the Chinese Government uses for that purpose are altogether unique and developed and sold by Chinese companies.

Mr. Chairman, you referred in your opening statement to other companies which do provide specialized security products and which Cisco has not. Our technology has helped connect the world in an unprecedented fashion. Perhaps the most vivid example of this in China is the response to last week's earthquake. Within minutes, pictures and videos from the region were online, and contrast that with the situation in Tangshan 32 years ago when the world received no official confirmation for months that a quarter of a million people had been killed in a huge earthquake. Today, more than 220 million Internet users in China are testimony to the ability of the average citizen to find information which has been dramatically expanded.

But the phenomenon of Internet censorship is, nonetheless, a global issue. Many governments around the world do not share our principles even as the Internet facilitates unprecedented communication. Around the world, governments do try to block citizen access to information. But Cisco complies with all U.S. regulations informed by human rights concerns which control sale of our products.

The policy responses that the Senate must consider with regard to the Internet and censorship are complex. Among the questions we have historically raised are: Has the Internet helped spread a dramatic access to information in regions where content is, nonetheless, subject to limitations? And if countries that engage in censorship are to be denied U.S. Internet technology, will those countries establish a closed Internet of their own, thereby enforcing the Virtual Curtain that Mr. Ganesan referred to?

In conclusion, Mr. Chairman, I have read and thought a lot about these important and difficult issues, and I agree with experts, including many human rights activists, who are of the view that engagement with China and other nations is more likely to lead to positive change than isolation. I also believe, having worked in the information technology sector for decades, that the Internet is one of the greatest contributors to positive change and that we should do whatever we can to make as much information available to as many people as possible. This can be accomplished through an Internet that is maintained as one global system built to global standards. I believe the U.S. Government for more than 30 years

has pursued a consistent and sensible policy, and the fact that the Internet is robust in China is a powerful testament to that fact.

Thank you again for inviting us to appear today before the Subcommittee.

[The prepared statement of Mr. Chandler appears as a submission for the record.]

Chairman DURBIN. Thanks, Mr. Chandler.

Our final witness is Dr. Shiyu Zhou. Dr. Zhou is the Deputy Director of the Global Internet Freedom Consortium, an organization that creates software that allows citizens in repressive countries to break through firewalls and freely access the Internet. Dr. Zhou is the Vice President of New Tang Dynasty Television and an adjunct professor at Rutgers University's Computer Science Department. He was previously on the faculty at the University of Pennsylvania.

Dr. Zhou, thank you for being here today, and please proceed.

STATEMENT OF SHIYU ZHOU, DEPUTY DIRECTOR, GLOBAL INTERNET FREEDOM CONSORTIUM, BETHESDA, MARYLAND

Mr. ZHOU. Mr. Chairman, Ranking Member Coburn, I am proud to stand before you today on behalf of the Global Internet Freedom Consortium, a small team of dedicated volunteers connected through their common practice of Falun Gong, who have come together to work for the cause of Internet freedom. We constantly battle tens of thousands of Internet monitors and censors around the world so that millions of citizens inside repressive societies may safely communicate online and access websites related to human rights, freedom, and democracy. These men and women maintain operations out of their own pockets, but provide their products and support services to the citizens of closed societies entirely free of charge.

The consortium has run the world's largest anti-censorship operation since 2000. Our services currently accommodate an estimated 95 percent of the total anti-censorship traffic in closed societies around the world and are used daily by millions of users. As of January 2008, the top five censoring countries with the most daily hits to our anti-censorship systems are: China, 194.4 million hits per day; Iran, 74.8 million hits per day; Saudi Arabia, 8.4 million hits per day; United Arab Emirates, 8 million hits per day; Syria, 2.8 million hits per day. And there are also users from many more closed societies, such as Cuba, Egypt, Sudan, and Vietnam. It has been transforming the closed society in a peaceful but powerful way that must not be underestimated.

Our tools have also been of benefit to U.S.-based organizations such as Human Rights in China, Voice of America, and Radio Free Asia, and even companies like Google and Yahoo!, who self-censor, since we bring the uncensored version of their services into closed societies. We have witnessed firsthand the effectiveness of anti-censorship technologies in improving information freedom for people in closed societies. During the democratic movements in Burma in late August 2007, our anti-censorship portals experienced a threefold increase in average daily hits from IP addresses originating in side Burma. After the protests broke out in Tibet on March the 10th of this year, there was a fourfold increase in the number of daily hits to our portals from Tibet, with Tibetans desperately try-

ing to send out information about the crackdown by Chinese authorities. Our anti-censorship tools are now one of the Tibetans' few remaining links to the outside world.

At the same time that we are battling the censors for the freedom of the people in closed societies, we are, unfortunately, finding strong indication that companies such as Cisco located in free societies may be involved in helping the Chinese security agencies monitor and censor the Internet, and persecute and prosecute Chinese citizens.

In a 2002 Cisco China PowerPoint presentation entitled "An Overview of [China's] Public Security Industry," now in our possession, a Cisco China official in the Government Business Department listed the Golden Shield Project, the host project of China's Great Firewall, as one of Cisco's major target customers. In this document, which apparently lays out the marketing strategy for Cisco China to sell products to the Chinese Security Police, one of the main objectives of the Golden Shield was to "combat the 'Falun Gong' evil cult," parroting the rhetoric of the Chinese authorities used to persecute Falun Gong.

In the presentation page headed "Cisco Opportunities [in the Golden Shield Project]," Cisco offers much more than just routers. It offers planning, construction, technical training, and operations maintenance for the Golden Shield. Our research shows that the infrastructure of China's Great Firewall coincides with the layout in Cisco China's PowerPoint presentation. Cisco can no longer assure Congress that Cisco China has not been and is not now an accomplice and partner in China's Internet repression and, whether directly or indirectly, its persecution of Falun Gong practitioners and other peaceful citizens in China.

Anti-censorship technology can allow the people in closed societies to be less subject to manipulation by an unscrupulous leadership. Winning people over to a more open and free system via the Internet could very well be a way to avoid future conflicts that can cost lives.

To our belief, reaching a critical mass of 10 percent of the 280 million Internet users in all closed societies will result in the avalanche effect that could lead to the fall of the censorship walls in closed societies.

The battle of Internet freedom is now boiling down to the battle of resources. The consortium has the know-how, experience, and capabilities needed to reach the critical mass in this coming year with just modest funding. We hope and trust the Senate and the Congress will grasp with what we believe to be a historic opportunity. Only when the U.S. shows more determination to keep the Internet open than the closed societies will to seal it off can there be the hope of information freedom and democracy for the citizens in all closed societies and a more peaceful tomorrow for all of mankind.

Thank you.

[The prepared statement of Mr. Zhou appears as a submission for the record.]

Chairman DURBIN. Dr. Zhou, thank you very much.

Senator Coburn has another hearing that he has to attend, and I am going to allow him to ask questions first so that he can put

some questions on the record, and both of us will reserve the right, as will the other members of the Committee, to submit written questions after this hearing.

Senator Coburn?

Senator COBURN. Thank you, Mr. Chairman, for your graciousness.

Mr. Chandler, how do you respond to what Mr. Zhou just said? He has outlined not just the sales of equipment, but the management and advisement and counseling and training on how to affect censorship by the Chinese.

Mr. CHANDLER. Thank you. Once again I would reiterate the respect I have for the efforts that he undertakes to allow access to information that censors would otherwise preclude access to.

I was appalled when I saw the line in the slides and very disappointed to see it even as a quote from a government official. There were several pages in the presentation which said here are the government's goals with this project, the government's goals with the next project. And the Golden Shield section has quite a few pages in the presentation devoted to different aspects of what they were trying to accomplish, including illegal drug interdiction, traffic management, and so forth.

The description in there had to do with what generally involves network planning and layout, which is something you do when you sell routing and switching equipment. We do provide service for our equipment so that it can be fixed if it is broken, and that is the type of service that we provide, technical service so that people understand how to use the equipment.

The only equipment that has been sold as a result of that is routing and switching equipment for essentially office automation and internal purposes within the Public Security Bureau. It has been a relatively small amount, I think, in the year after that presentation was made, and, again, we are talking about something that was 6 years ago. I think there was approximately $10 million of sales, and, again, office automation equipment more than anything else—in fact, exclusively.

That is the nature of the implementation. There was nothing there that had to do with censorship, none of this kind of strong security products that the Chairman referred to in his opening remarks that would facilitate that type of communication interception. And I would point out just by way of example that when an issue arose a couple of years ago regarding someone who was arrested as a result of online posting, that was not done by the government because they were able to receive information from Cisco products. They had to go to the service provider in question and try to identify the individual by name. We are providing generic routing and switching equipment in these instances that we do not think facilitates the types of activities that I know are very troublesome to Dr. Zhou and to us as well.

Senator COBURN. Dr. Zhou, the references to the 2002 presentation, do you have information outside of that 2002 presentation that would lead you to conclude that the facts are otherwise from what Mr. Chandler stated?

Mr. ZHOU. Yes, we have. Actually, we have just submitted another document to the Subcommittee this morning. It is apparently

a sales pitch presentation by the same Cisco-China person who made the first 2002 document, to the public security police in China, showing how to use Cisco equipment to construct the Golden Shield Project in different cities and provinces, including Beijing.

Senator COBURN. To Mr. Chandler's point, though, even though they built it, they still have an ISP that they have to go through. Is that correct?

Mr. ZHOU. I am sorry. The—

Senator COBURN. Well, you can build it, but there is still an Internet service provider that people are using. So will they not and still have to use the complicit help of an ISP with which to identify someone?

Mr. ZHOU. Well, Cisco's routers have—it is a supercomputer. It has various functions. And the censorship, which is the thing that we are concerned most about, happens at the national gateway level, and so they can monitor, they can do content filtering, and they can do a hijacking of the DNS, and also they can do IP blocking so people cannot see websites.

And in regard to the monitoring system you mentioned, Cisco also has other equipment, including voice and image recognition and other things, that could be used. And if you want to track down the users of certain going to certain IP addresses, well, so there are many ways to do that, and so there are other companies who are doing this, and Cisco is one of the major companies.

Senator COBURN. All right. Our first two witnesses talked about using trade and enhancing our USTR in terms of our approach to censorship. Why not just, Dr. Zhou—rather than give it to a bureaucrat and create an anti-censorship center where we, in fact, make it so hard for them to censor that they give up, that he wins, that we get over the critical mass rather than do it through the bureaucratic maze? It obviously has not worked in the past on several other issues in China in terms of both the State Department and the USTR. Why would you make—why would you think that that would work through the Trade Representative or the State Department that China is going to change its policy?

Ms. WONG. I will take that, because I think we have a number of recommendations that are in my testimony. And let me explain.

I think the USTR is an important step. I think it is important to recognize that freedom of information on the Internet is a trade issue and that we can use that with other countries as we negotiate those agreements. But having said that, Senator, you are absolutely right. It is not a silver bullet. The Government has many tools in its toolbox, and we would actually encourage them to use a variety of them.

We think the USTR one is a good one. We think greater prominence and authority given to the State Department would also be very, very helpful in our experience in talking to countries. Particularly there is a second generation of countries that are coming online, and they do not have the same values that we do on freedom of expression or governance, and to have State Department officials who could engage them on that level would be enormously effective.

Also, as a company, we support the development of tools that are intended to get around censorship of the Internet. We do that in a couple of ways, both directly supporting developers in that area, and also providing a code base for building on top of. There are a number of things, I think, that can be done. The USTR is one of them.

Senator COBURN. Mr. Samway, do you want to comment on that?

Mr. SAMWAY. Senator, that is a very good question. We are a technology company, and certainly technology is part of the solution, and we are going to explore Dr. Zhou's organization and the technology offered. At the same time, it is also a human problem. It is a company challenge, and we are taking on the challenge at Yahoo! to build internal capacity to make responsible decisions on human rights.

There is also an important role for Government to play, and we agree not only with using trade, but all the other, as Ms. Wong said, tools in the U.S. Government's toolbox to emphasize that Internet freedom is a global priority.

Senator COBURN. It may be my lack of knowledge, but I think that is already our policy. Is it not already our policy at the State Department?

Ms. WONG. I believe there is a freedom-of-expression component to the State Department's mandate. I think in our experience they have been very helpful with us in some instances with some governments. My sense is they could use greater resourcing, greater prioritization.

Senator COBURN. OK. Thank you.

Mr. Ganesan, what is your thought about what Dr. Zhou does and the likelihood that whether we have a Government-mandated committee look at this or a voluntary organization from industry look at it and have a tool up here that is above the box versus what he is doing below the box, which do you think ultimately is going to be more effective?

Mr. GANESAN. Thank you. I actually think all of them will. I think that you do need to foster new technologies to get around firewalls and to get around censorship and to help people protect their privacy.

At the same time, I think that Government can be more aggressive. The State Department, I believe, has a Global Internet Task Force, which it has now launched twice, I think, and so there is a lack of clarity as to what its ultimate purpose and its overall strategy is, and I think that that could be addressed. And I think trade policy could be useful, but it is important to bear in mind that these are long-term fixes and diplomatic fixes. The immediate fix may be fostering new technologies and, most importantly, getting leadership companies to do the right things. And the balance that we want to strike between a voluntary and mandatory initiative is that some things can be done voluntarily, providing the public has the assurance that what people say they are doing is actually done.

But then there are going to be cases, like China or others, where the Government is just too good at picking off individual companies or pressuring them to do the wrong thing, in which case rules need to be changed so that they have a backstop which helps them move beyond that into something else.

Senator COBURN. Somewhat they are using their purchasing power to be able to influence what is happened.

One last question, and I will submit the rest of mine for the record. Google participates in China, but you do not offer Gmail. Why not? Turn your microphone on, please.

Ms. WONG. When we launched our services in 2006, we thought very carefully about how we could do that in a way that we would be maximizing the availability of information in China while also protecting user services. And we took a lot of lessons from the examples of companies that went before us.

One of the decisions we made was that we did not want to host Gmail or Blogger or services that would include confidential, sensitive information that we might be required to provide to the Chinese Government. So the services that we currently offer in China include our search services, a map service, a local business service, and some others.

Senator COBURN. But there other countries that have repressive regimes and Internet censorship where you offer Gmail. How is it you can do that in those countries and not in China?

Ms. WONG. Because of the nature of how we have seen the government use information, we were particularly concerned about China. We do offer Gmail in other countries. Before we launch in countries, we do try to—we do an assessment of those countries in terms of both our risk of being compelled to produce information in those countries as well as what the government structures in those countries look like.

Senator COBURN. All right. Thank you.

Thank you very much, Mr. Chairman.

Chairman DURBIN. Thank you, Senator Coburn. I understand you have to leave and you will submit some questions for the record. We are joined by Senator Whitehouse, and I would like to ask first some questions related to this Cisco PowerPoint, Mr. Chandler.

First, do you know the person who was responsible for this PowerPoint presentation, which made the negative reference to Falun Gong and talked about using Cisco's resources to train the Chinese Government in censorship and repression?

Mr. CHANDLER. Well, first of all, I do not know him. I have never met him. I have never spoken with him. He is not a manager. He has nobody who reports to him. He is a first-level employee. I think he is four or five levels down in the Chinese—

Chairman DURBIN. Does he still work for Cisco?

Mr. CHANDLER. Yes, he does. The document did not propose on behalf of Cisco that Cisco combat in any way or adopt any of the government's goals. It simply listed what the government's goals were, and there were several pages within the document that do that. You will note on the chart that Mr. Zogby is holding up right now that the first two bullets from this government statement were crack down on Internet crimes and ensure security in services of public Internet, which are fairly straightforward goals for network administrators.

There was not a proposal whatsoever in the Cisco document that Cisco be involved in censorship or monitoring. And, interestingly, just to draw on something that Professor Zhou said, the censorship

and monitoring that would occur would not be within that ministry, apparently, but as Dr. Zhou said, at the gateways where information comes in and out. And so that project that was referred to there did not seem to have any censorship or monitoring aspect to it with respect to anything Cisco could provide.

Chairman DURBIN. Does this person still work for Cisco?

Mr. CHANDLER. Yes, he does. I would note, by the way, that we have no video recognition, and the only voice recognition we have is so people can dial by picking up a phone and asking for their voice mail. So that is just not our product either.

Chairman DURBIN. Now that this document has been made public, what efforts will your company make to clarify your position relative to Falun Gong and this type of conduct?

Mr. CHANDLER. Well, first of all, the document is a 6-year-old description of the Chinese public safety organizations and how they were laying out their network plans based on what government officials were saying about them.

With respect to our position, as I said in my testimony, the views of the government officials cited in it were not Cisco's views then; they are not Cisco's views now. That was an internal document describing the government's goals that was used internally among Cisco employees, and but for the fact that it was put on the record here, would never have been identified with Cisco in any case, whatever our view.

Chairman DURBIN. What internal systems or written policies does Cisco have so that your employees in China, or any other place, do not assist a government's efforts at censorship and repression?

Mr. CHANDLER. Well, it goes to the nature of our products. The principal thing that we do that is beneficial in that respect is that our products are built to global standards, and we sell the same products globally. So we do not customize them for those types of purposes in any way. And that is the fundamental principle that we have that applies globally. We do have 65,000 employees the world over; documents are generated every day describing the capabilities of our products. And it was inappropriate for him to include a political goal that—

Chairman DURBIN. As a matter of record, I accept that, but my question was specific.

Mr. CHANDLER. Yes.

Chairman DURBIN. What internal systems or written policies do you have to make it clear to your employees not to engage in conduct that supports the Chinese Government's censorship and repression?

Mr. CHANDLER. We have a written, extensive code of conduct that refers to the way our products are to be used, what the aspirations of the company are, and we also have a corporate social responsibility organization that clearly sets forth in our annual review of that what the company's support is for human rights globally, including the power of the Internet to do that. And employees who would customize our products in such a way as to undermine human rights would not be consistent with the code of conduct that we have.

Chairman DURBIN. Does your company inform government clients, in writing or otherwise, that they will not assist in efforts toward censorship and repression?

Mr. CHANDLER. Given that our products do not do that, I am not sure the nexus for providing that kind of statement to a government in that the products that we provide as global standardized products for routing and switching of information simply are not applicable to that purpose.

Chairman DURBIN. Dr. Zhou, would you like to react to Mr. Chandler's comments?

Mr. ZHOU. Yes, Mr. Chairman. We should consider a normal business procedure that Cisco and other companies use to do business with China, in which we have pre-sales services and also post-sales services.

In pre-sales services, you get the objectives of your client and make a proposal to them. Like in this PowerPoint, it tells Cisco people about the objectives of the Chinese police force and how to market Cisco products to the Chinese, including how to "combat Falun Gong."

After the sales, you have post-sales services by implementing the solution to achieve the objectives. That includes the (lower-level) design, customization, testing, implementation, plus training, maintenance, etc.

Cisco routers are supercomputers. They can be used as a toy, but they can also be made into a A-bomb. It completely depends on the objectives of the client.

Cisco can design it purposefully to accommodate the needs of the client, and that is what the other document submitted to the Subcommittee is doing—Cisco made it into an A-bomb to accommodate whatever the Golden Shield Project needs.

Chairman DURBIN. I might say for the record that the other document you have referred to was given to the Committee about 5 minutes before the hearing in Chinese.

Mr. ZHOU. Right.

Chairman DURBIN. And so—

Mr. ZHOU. The English. The English.

Chairman DURBIN. In English as well?

Some of it is translated and some of it is not. We are still working on the translation, so I thank you for that.

Mr. Chandler, I want to give you the last word on this, and then I want to ask some other questions, if I might. I would like to add to Dr. Zhou's comments.

Mr. CHANDLER. Sure. I think that there are several things that I think we can do and that are relevant and positive in this respect. Cisco does support the goals of the Global Online Freedom Act to promote freedom of expression on the Internet and also to protect U.S. businesses from coercion by repressive authoritarian foreign governments. In particular, we support section 104 that would establish an Office of Global Internet Freedom in the Department of State. We support restrictions on the ability of companies to locate within an Internet-restricting country electronic communications that include personally identifiable information, which we generally do not do in any case. And, finally, we also support title III, which would require the Secretary of Commerce, in con-

junction with the State Department, to conduct a feasibility study for the development of export license requirements regarding export of any items to an end user in an Internet-restricting country that would facilitate substantial restrictions on Internet freedom.

We comply fully with the U.S. laws that exist today, including the Foreign Relations Authorization Act that was enacted in 1990 and puts specific limitations on supply of certain crime control equipment to Chinese Government agencies. There is a lot that can be done.

Chairman DURBIN. I am going to submit a question for the record relative to Commerce Department regulations on equipment that I hope you will have a chance to respond to through your company. And I would like to ask the others a few questions. I do not know if you have a few minutes, Senator Whitehouse. Do you?

Senator WHITEHOUSE. I am supposed to be on the floor shortly.

Chairman DURBIN. Oh, well, go ahead. Senator Whitehouse, why don't you go ahead and ask questions, and I will return after you.

Senator WHITEHOUSE. I would appreciate it, Mr. Chairman. I will be quite brief. First of all, I want to thank you for holding this hearing, and I think particularly the emphasis on representing basic human freedoms and rights in our trade policies that Ms. Wong brought up and that has been discussed in this hearing is particularly important. I have been pressing in my brief time in the Senate for our trade policies to reflect basic things, like honoring property rights in countries that we have trade relationships with, honoring free press, and I think the discussion about honoring Internet openness and neutrality has been helpful to me in informing those views and other areas where I think our trade policies could effectively reflect our values better than they do.

With respect to the American companies that are here before us today, let me ask you this: Are you selling products or services in China that are different than your standard products that have been customized or tailored—I think Dr. Zhou used the word "customized"—in any way to facilitate the repressive efforts of the Chinese regime? And I ask that question because it is a different question for me if, you know, we are selling a Ford car that is a standard Ford car and the Chinese police are using it for repressive purposes. That really does not necessarily trail back to the responsibility or culpability of the Ford Motor Company. On the other hand, if the American equipment is being tailored to support the repressive efforts in any way, that seems to me to raise a different question.

So I would ask each of you, I guess Mr. Chandler, Mr. Samway, and Ms. Wong, if you could answer that for your respective companies.

Mr. CHANDLER. No, we do not.

Mr. SAMWAY. Thank you, Senator Whitehouse. We do not sell equipment. The services that we offer on yahoo.com are available to Internet users all over the world in the same form—

Senator WHITEHOUSE. The same whether you are signing on France or India or U.S. or China?

Mr. SAMWAY. That is correct, assuming you have access and it is not blocked. The local subsidiaries of any company will be required to comply with local laws, and that would be the case with

the companies that we no longer control but that is run by Ali Baba and called Yahoo! China. And we, like you, believe deeply in free expression and certainly in privacy. Those are our founding principles.

Senator WHITEHOUSE. Ms. Wong?

Ms. WONG. We offer a global service, which is our google.com service, the service you can access here in the United States. That is available throughout the world, including in China, and what we found prior to 2006, when we first launched our local service on google.cn in China, is that google.com would be frequently blocked, completely unaccessible to the people of China. And so after much discussion by our senior executives about how to still be able to provide meaningful information in China, we decided to offer a localized version on our google.cn domain, which is, in fact, compliant with Chinese law pursuant to our license requirements.

Senator WHITEHOUSE. Do you do that in other countries as well?

Ms. WONG. We do, actually. So our strategy in China and globally is to make as much information available as possible, and if information has to be removed, to be transparent with our users about that. So, for example, in Germany, which prohibits Nazi propaganda material, we will remove at the request of the government that type of material from our dot-de, our German local domain. That is the same, for example, in Canada, which has a law that protects certain groups and prohibits hate speech. Upon request, we will also remove that sort of information when found on our dot-ca, our local Canadian domain.

In China, we likewise do the same and, candidly, with great reservation. That is why it took us so long to get into China in the first place. But we do comply with the local laws there.

Senator WHITEHOUSE. Thank you very much.

Thank you, Chairman.

Chairman DURBIN. I want to followup, and if you could—I do not know if you have to leave immediately, Senator Whitehouse, but if you could show the two charts here from google.cn and google.com, we tried to find a reference here to something very generic, and so we decided it would be images—is that the first one? This is on Human Rights Watch, which, of course, Mr. Ganesan is here representing. And you will notice on the one on the right, when you log in Human Rights Watch, what is available on Google, and over here on the Chinese side, I think if I can find the translation here, what they have to say about it is—the cn site says "cannot find the Web page matching your inquiry." So if you are looking for Human Rights Watch through google.cn, they basically say they do not know what you are talking about. But if you go to google.com and make the same request, there are some 35,000 entries that are available to you.

Ms. Wong, is that what you meant earlier when you said you offered both of these?

Ms. WONG. That is right. We do offer both of those. So google.com is always made available except when the Chinese Government itself decides to block us through its Great Firewall.

Chairman DURBIN. Let me show one other example, if I can, and this one is photo images that are available. This is through Yahoo!, and you will notice on the right, if you would type in "Tiananmen,"

you will receive Yahoo! images which reflect what happened in Tiananmen Square, the historic events in Tiananmen Square. However, if you go through the Chinese site here, you will notice that there are a lot of tourist postcard images of Tiananmen Square. It is a dramatically different presentation. This is what I believe the people in China are likely to see. They are basically being excluded from seeing the reality of what actually happened in Tiananmen Square. We use these just as examples so you understand what this is about in terms of drawing these lines.

I am trying to step back here and put myself in your position for a moment in terms of world competition. I start this with the knowledge that 12 to 13 years ago, I was following very closely what was happening in the Baltic States. My mother was born in Lithuania, so I watched closely as they tried to separate from the Soviet Union and bring democracy.

The thing that saved the Baltic revolution in Lithuania was the fax machine. It is hard to believe in this day and age that would be true, but the Soviets could not stop the fax machines. And they were humming 24 hours a day with information coming out of Lithuania and the Baltic States about what was really happening, because you could not find out on the ground, from official sources or otherwise, what was happening. So that very primitive and early technology I think had a lot to do with democracy coming when it did to the Baltic States.

So my notion when we got into the debate about China and its free trade agreement was that there was no way that a central authority, a government in China, could control the glow of all those modems across China, that eventually that information would overwhelm any government's effort at control. And I think that goes to the heart of why we are here today.

There are two issues as I see it, and one is the complicity or cooperation of American companies in limiting information, because of government censorship or otherwise, to clients in foreign countries. And the second part we have not touched on but that we need to—I referred to it in my opening—is the privacy of individuals and the cooperation of American companies in identifying individuals who will then subsequently be arrested, charged, and imprisoned for seeking information or sharing information on the Internet.

It strikes me there are two things here, the censorship policy and the privacy policy, that we have to ask about. And the obvious question is: Can we, should we, establish standards for American companies involved in global commerce when it comes to these two things? Should we declare it wrong for an American company to in any way cooperate with censorship and repression?

Ms. Wong, what do you think?

Ms. WONG. So you know, let me talk a little bit about the process that we undertook in going into China, which is prior to 2006 and launching our dot-cn product, which is censored. We found ourselves completely out of that market. For unexplainable reasons google.com would be blocked, with nothing getting through in China, much less politically sensitive material. And so what our senior executives wrestled with was would it be better to be there and be engaged and offer some level of information rather than to

be completely blocked for reasons that we are completely unable to control?

And the most persuasive people that we spoke to when we were wrestling with that were actually Chinese users in China who used the Internet extensively. They said, "You will do more for us by being here than by staying out." The classic diplomatic question of engagement, which is—

Chairman DURBIN. I think I heard this same argument when it came to apartheid in South Africa, as to—

Ms. WONG. Well, let me explain—

Chairman DURBIN.—whether we should impose sanctions, have normal relationships, or—and there were some who argued, well, wait a minute, if the United States does not trade with South Africa, the South African people will not have as many products to buy and it will be hurting them, and they are not the culprits. It is the government.

Ms. WONG. And that is certainly a valid argument in that case. Here is what our experience has been, and the reason why they told us to be there is that they believe that we would provide competitive pressure to cause other companies to do better. So let me give you an example of how that is.

When we went into China, we decided that if we were going to remove search results, we would have a notice at the bottom of the page. The notice basically says there are some search results which are not appearing because of local rules, laws, or regulations. There was no other search engine in China doing it at the time that we went into China. After we did it, the other major search engines in China are now having a similar type of notice. That is a level of transparency that lets Chinese users know, even if our U.S. service is blocked, that something is missing in their search results. And we think that that is real evidence that we being there has moved things in the right direction. It is imperfect, and we know that. But we do think that something about being there is right.

One more example, because I think that it is appropriate that we focus on the very difficult issues of political censorship in China, which we disagree with completely. Having said that, there is also something about being there, about having our open search box for Chinese users to go and ask any question they want, to exercise the muscle of asking any question they want and seeing what results they get back. That in itself, we think, makes it worthwhile for us to have a presence there.

Chairman DURBIN. Mr. Samway, I would like your response to the same question.

Mr. SAMWAY. Thank you, Mr. Chairman. I also appreciate the opportunity now to talk a bit about the example that you raised on Tiananmen Square. Just below the surface in places like China, there is incredibly robust discussion, open discussion, and access to various subjects, whether they are local corruption, environmental issues, health issues. The recent earthquake in the Sichuan province is an example of how the Internet is transforming society in places like China.

Senator Coburn made a reference that I thought was especially powerful when he noted that information itself is power, and that is what is available today more than ever before to Chinese citizens

despite the best efforts of the government. We believe deeply in free expression and open access to information, and like other companies, we also believe philosophically that engagement is good.

Chairman DURBIN. So Dr. Zhou in his testimony, his full testimony, underscored the consequences of public censorship in another area we have not discussed—public health. He noted that the Chinese Government detained many people who attempted to disseminate information about the SARS epidemic in 2004. In 2006, Amnesty International testified before Congress that over 100 people had been arrested for "spreading rumors" about the SARS outbreak, which obviously affected people all over the world.

So I guess my question to you is: You talk about the positive opportunities where the Internet can provide information, much like the early fax machines I referred to, that otherwise might not have been available. But how do you deal with the other side of that coin that Dr. Zhou raised? That is, when you are asked to be complicit through your companies in restricting the flow of information for the public good and public health, aren't your hands a little dirty at the end of the day if you participate in that? Mr. Samway?

Mr. SAMWAY. Well, Senator, it certainly is troubling, and we are troubled by the actions of the Chinese Government with respect to their own citizens. We take responsibility. We have learned valuable lessons, probably more than any other company in the room, and we are taking those lessons and implying them, taking individual steps and collective steps. We have been working, for example, as a participant in this broad-based global human rights dialog. Mr. Ganesan is one of the leading participants for the human rights groups. We believe collective action is critical. We also believe individual steps, independent of what we can do as a group of companies, are critical. We are taking this multi-pronged approach because we have learned important lessons.

We also believe, as you know, Mr. Chairman, there is an inherent tension, there is always a tension in going into these emerging markets between opening up, allowing more access to be available, and what the government can do to try to control that access. And the SARS example I think is a very good one. At the end of the day, the government was unable to stop the tide of the flow of information, I believe, with respect to SARS. They tried to contain the health epidemic which threatened to become a global one, and ultimately, communication and awareness of the issue required them, essentially forced them, to come out into the open about the challenge.

Chairman DURBIN. Before we go into the second aspect here, the right of privacy of individuals, I want to stay on this topic and let Mr. Ganesan and Dr. Zhou comment on what you have heard. From what we are hearing from Google and Yahoo!, it is better that we are there than not being there. The people would rather have us there in the country even if there is censorship. We are notifying people that what we put on the Internet is censored. And isn't it at the end of the day a better policy to engage rather than to step back and disengage? Mr. Ganesan?

Mr. GANESAN. Thank you. Well, I think that we all believe that the free flow of information is a good thing, wherever it is. But I

would draw a very strong distinction between what the companies are saying and what is actually happening.

There is censorship that a government imposes by taking down a website or blocking Internet access. Then there is censorship that a company does by its own discretion, which is what is happening with search engines in China. There is the firewall, and then there is the choice of companies to censor. And the disclaimer, which is now about 2 years old—because Google did talk about it at the first hearings on the Internet before—is basically telling people that we censor. It is not saying we are reducing censorship, which is a separate issue. And what we have tried to do, both in terms of regulation and pushing for legislation, as well as through a voluntary initiative, is saying disclosing censorship is not enough, but actually actively trying to reduce it to where your minimum level is whatever the government says it is. Nobody is going to find a company culpable if a government does like what they did in Burma in September 2007, which is physically disconnect telecommunications lines to prevent access. But where people are going to look askance at a company is when they choose what to censor and they decide, in anticipation of what the government wants, what to censor. And what we are trying to do is get at that problem, because we know governments are going to try to restrict the flow of information, but what we would like to see is companies go beyond the disclaimer and actually reduce the amount of censorship going through.

Chairman DURBIN. I am going to ask you about the code of conduct, and I want to come back to the Foreign Corrupt Practices Act, but first code of conduct. Why has this taken so long? Which companies are dragging their feet? What is the issue that has stopped our American companies from establishing a code of conduct so that we at least can say we are not being hypocritical, the values we have as Americans are reflected in our corporate behavior?

Mr. GANESAN. The fundamental issue is a resistance to having some third party come in and actually attest that the companies are doing what they say they are doing. And I think the resistance from that is somewhat reflective—I think companies in general do not want to see third-party oversight—and also misguided, because people forget that the reason we are calling for a code of conduct and independent monitoring is because when the companies were given discretion on censorship and user privacy, they did not perform that great. That is why we are here today. That is why we were here 2 years ago and the like.

So now we need somebody else to step in just to attest to the public that, hey, this process is in place, and if they commit to doing this, we can actually show you in some way that they are actually implementing these things, because the code of conduct is not to assuage Human Rights Watch or anyone else; it is to assuage a 20-something blogger in a country that wants to speak out about his government, and he needs to know that he is not making a Faustian bargain with a U.S. company, which is in exchange for posting information that might be problematic for a government, that he is not going to do it on a service that actually turns that information over to a government or stops it from being posted.

Chairman DURBIN. So, Ms. Wong, Mr. Samway, why won't you agree to independent monitoring? Why is this code of conduct taking so long?

Ms. WONG. Well, Mr. Chairman, we, in fact, were one of the founding companies to begin this discussion, and we are deeply committed to it. We have been at every meeting. We have been moving it along. And we agree, the 18 months has been a long process.

Let me say two things very clearly. We would support an external audit. We are very optimistic that it will be finalized. Let me also say what our measure of success for this process would be. For us, the importance of having all of the companies and the addition of the human rights groups is not necessarily about looking at whether the companies are being held accountable to their processes. The point of having all of the companies stand together on important principles—like freedom of expression, requiring rule of law, you know, doing an assessment of the countries we go into—is so that the companies would stand together against the governments and hold the governments accountable. The measure of success of this process is whether we walk away with an ability to put pressure on governments to do the right thing. That is the problem that we are facing.

Chairman DURBIN. Mr. Samway, are you agreed to independent monitoring, external audits? Will Yahoo! sign up for that?

Mr. SAMWAY. Thank you, Mr. Chairman. I will tell you what I have said to Mr. Ganesan in our private meetings without, I think, breaking the trust of the group. We unequivocally support independent assessment of company activities.

Chairman DURBIN. Looks like we have an agreement, Mr. Ganesan. Bring out the papers and let's sign up.

So what is the obstacle? Why is this still going on for 18 months, the negotiations over a code of conduct?

Mr. SAMWAY. At Yahoo! we are ready to move forward, as I mentioned in my testimony.

Chairman DURBIN. Well, I hope that within the next 48 hours we will have an announcement. That would be terrific.

Dr. Zhou, you have heard the companies explain that they believe they are doing the right thing by at least being in China, even if they are subject to the censorship standards and policies of that country. What is your reaction?

Mr. ZHOU. Mr. Chairman, I would like to make two points. First, for companies like Google and Yahoo!, I would say that their self-censorship in China can be more damaging than other kinds of censorship. This is because for Chinese people in such a closed society, they take Google and Yahoo! as role models of freedom of information. When they look at their websites and find the information, they believe it is factual and unbiased. Therefore for those not-so-much politically conscious people, this is deceiving—they get the information from Baidu, and get it from Google and Yahoo!, they compare them and conclude that, well, they are the same thing and that is the truth.

The second point I want to make is that Google and Yahoo! do not have to bend their knees to enter China. They can just upright and walk into China by bringing down the firewall. They can

achieve this by either supporting companies like us or finding their own way.

Chairman DURBIN. Let me go to the second issue that I raised, the rights of the individual. Mr. Samway, it is my understanding that at the request of China, your company, Yahoo!, disclosed the identity of a person, Shi Tao, who was then later prosecuted, convicted, and imprisoned. Can you tell me, what kind of standards would Yahoo! use to decide that one of your customers should be subject to that sort of prosecution for what would be innocent conduct here in the United States?

Mr. SAMWAY. Let me begin, Mr. Chairman, by saying that it is deeply troubling that people have gone to jail as a result of some connection to our company. We have also tried to take steps specifically with Mr. Shi. In particular, we have settled a lawsuit. We have also announced the Human Rights Fund and have been working closely with Harry Wu, a noted activist and human rights dissident based here in Washington, to create this fund to provide humanitarian assistance for dissidents such as Mr. Shi and other dissidents who have been imprisoned for expressing their views online.

Chairman DURBIN. And so tomorrow if Yahoo! had a similar request from the Chinese Government to disclose the identity of someone who had been involved in what they considered to be illegal conduct or misconduct, what would your company do?

Mr. SAMWAY. Well, as you know, Mr. Chairman, we currently have an investment in a company that runs the day-to-day operations of Yahoo! China. That company complies with the law, as would any Chinese company. Again, we are deeply troubled by the consequences of the restrictions on access to information and also the attempts by the government to seek disclosure of data on its own users.

Chairman DURBIN. So you own 40 percent of the company, which if it received a request, I take it from what you said they would disclose the name of the person. Is that true?

Mr. SAMWAY. Mr. Chairman, you make a good point about compliance with the law, which any Chinese company would be required to do in this case. Frequently, sir, it is not the name of the person. There is a request that comes in for a user ID that is not always identifiable to the person him- or herself. But, again, to us it is deeply troubling, and as I mentioned, we take responsibility for our own actions. We have learned valuable lessons, and we also want to take concrete steps working with partners, working on our own, to make responsible decisions in the future, to be a leader in human rights.

And to give you one example, we currently conduct—and I think we may be the only company to publicly announce and commit to this—a human rights impact assessment before entering any market, and it covers the two pillars that you mentioned: free expression, which goes to censorship;, and user trust, which goes to privacy. We assess what the potential intersection points are with our products in the current human rights landscape in the country and design mitigation strategies to address those issues.

Chairman DURBIN. Well, I am still a little bit troubled by this, because as I understand what you have told me, it is that you have

enlisted Mr. Wu, who is widely respected, and others. You have made investments, dollar investments, in human rights funds to support the families of those who are imprisoned. And you are committed to human rights. But at least through the company that you own a 40-percent share of, you are going to have a booming business with your human rights assistance fund because as you turn over more and more Chinese who are using your product for prosecution, there will be more need for assistance for their families.

I am struggling with trying to reconcile here what your corporate goal is and your corporate image in this debate.

Mr. SAMWAY. Well, as I mentioned, Mr. Chairman, our founding principles include promoting access to information. With respect to Alibaba, we also have exerted our influence with respect to the free flow of information in China. And to give two examples, one relates to search disclosure, and that is, notice to users on all search pages of Yahoo! China that certain results do not appear. There is also a notice on the registration page of Yahoo! China that indicates that the product itself is subject to PRC law. Now, those are forms of influence that we have tried to exert. It is a complex relationship, certainly, and Yahoo! China makes its own decisions day to day, not at the request of our team at Yahoo! But certainly we can exert influence; we have and will continue to explore avenues to exert that influence with respect not just to censorship but to the privacy issue you raise.

Chairman DURBIN. Ms. Wong, how does Google deal with its so-called complex relationship when it comes to disclosing the identity of your users?

Ms. WONG. So we go through a similar struggle in terms of thinking through which countries we will enter and what services we will make available. And as I mentioned during my earlier testimony, in China we made a decision to launch only certain services. We do not offer Gmail or Blogger on our dot-cn, our Chinese service, specifically for the reason that we do not want to be in the position of potentially compromising someone engaged in political dissent.

Chairman DURBIN. So Google decided they would rather not do business in those areas which were most likely to be compromised by Chinese law.

Ms. WONG. That is correct.

Chairman DURBIN. Mr. Samway, Yahoo! decided they would do business but through another company, and let me ask you: Was there a sensitivity to this same issue? You realized you were walking into areas with e-mail and blogging most likely to be monitored and prosecuted by the Chinese Government, but decided for economic reasons to do it anyway?

Mr. SAMWAY. If I can give some context to the timeframe, we feel like we were Internet pioneers and moved in, in the late 1990s in the market, indeed before other companies even existed in the technology space. We moved into China to expand information, to expand the availability of information. We moved in at a time, as you know, Mr. Chairman, when the U.S. Congress was normalizing trade relations with China, encouraging not only American companies generally but American technology companies specifically to go into this market, to explore it. As a young company, but 5 years

old at the time, we entered this market—again, as a trailblazer, as a pioneer. And as I mentioned, we have learned tough and valuable lessons. We are also taking those lessons and enacting concrete steps to build capacity, not to gather a group of smart people around a table and figure out what the future of the Internet should look like, but building real infrastructure into the company's DNA so that we can make responsible decisions on human rights.

Chairman DURBIN. Ms. Wong, I want to make sure the record is complete here. I have talked to Mr. Samway about a company in which they have an investment. Google has an investment in Baidu, which is the largest Chinese search engine.

Ms. WONG. We do not have an investment in Baidu.

Chairman DURBIN. You do not?

Ms. WONG. No.

Chairman DURBIN. I am sorry. Do you have an investment in any other—

Ms. WONG. I believe we did previously and sold off that investment a few years ago. I can check that out for you.

Chairman DURBIN. OK. Let me ask, then, on the Foreign Corrupt Practices Act. Mr. Ganesan has raised that, and I do not know that it is a complete analogy, but it is an interesting analogy. In 1977, we passed a law, the Foreign Corrupt Practices Act, which is aimed at stopping U.S. participation in bribery and other corrupt practices of foreign governments. When the law was first proposed, it was criticized by the business community at the time. Congress recognized the importance of stopping American involvement in these practices that went against our values as a country. The Act has lessened U.S. involvement in supporting corruption around the world, and what is more, it led to several international agreements and conventions to stop bribery and corruption internationally. When we took the first step against this, much of the world was skeptical, but then followed suit.

So let me ask both Ms. Wong, Mr. Samway, and Mr. Chandler: Do you see Mr. Ganesan's suggestion that we should pursue something along the lines of the Foreign Corrupt Practices Act to be analogous to what we are discussing here? Is it a way for us to declare that certain practices of foreign governments are inconsistent with the values of our country and can even be prosecuted in our country? Mr. Samway?

Mr. SAMWAY. Thank you, Mr. Chairman. I have to admit that I am not expert enough on the Foreign Corrupt Practices Act itself to know the details to be able to compare. I will say that I think there are four important points in addressing this issue, one of which gets to the point you make on legislation.

The first is for the government, the U.S. Government, collectively for governments around the world, to make Internet freedom a priority. There are different ways to do that. Again, governments have different tools in the toolbox to do that.

The second way is for companies to build capacity on their own. We do not need to wait for a collective process, and I agree, independent assessment has been a point that has held us up recently. At the same time, this most meaningful part of collective action is really about companies building capacity to make responsible deci-

sions. Independent assessment is important. There are clear practical limitations. That is exactly what we struggle with, what we have been focused on most intensively, I would say, in the past few months.

The third area where we can really create change is around collective action, and that is getting to yes in this global code of conduct, where we have a collaborative process with companies, human rights groups, academics sharing, learning, and helping to understand the challenges of the problem.

The fourth area, which I think gets to your point, Mr. Chairman, is legislation. We support backstop legislation, something that protects U.S. companies, but not legislation that puts us in the untenable position of having to choose to violate a local law or choose to violate U.S. law. That is not sustainable or tenable for a U.S. company, and then we get back to the philosophical debate on engagement. And a company will ultimately have to choose not to go in.

We support engagement. We support legislation that allows companies to act responsibly, that has appropriate limitations, and a clear enough depth of understanding of what the challenges are we face on the ground.

Chairman DURBIN. So, Mr. Ganesan, doesn't that get to the crux of it here? When it came to foreign corrupt practices, we were dealing with issues that were nominally criminal already in the countries where they were being performed. In this situation, we are dealing with practices, such as censorship, which are nominally legal in the countries where we are finding it. Isn't that a critical difference?

Mr. GANESAN. It is a difference, but there are ways to deal with it. I mean, there are two elements of the Foreign Corrupt Practices Act. One is punishing someone for the act committed, and the other one—and this is what is important in this context—is ensuring that the companies have the systems or the capacity in place to prevent that act from occurring. So say we take user privacy and freedom of expression, non- censorship. We can certainly devise standards, in the voluntary process or otherwise, on what a company should be doing to reduce or minimize the risk of that happening, just like the Foreign Corrupt Practices Act does with bribery. And we can legislate in a way that companies are bound to show that they are taking those steps internally to reduce censorship and reduce the risk to user privacy.

Now, on the flip side, what happens when a company is in conflict with the local law? The Global Online Freedom Act tries to set out a process in which a questionable request from an Internet-restricting country, as designated by the Act and designated by the government authority within the Act, will—instead of having the company have to say no to that government, it sets out a process where the U.S. Government steps in and deals with it in a diplomatic manner.

So, in other words, in a sense it raises the transaction cost for the repressive government because now instead of bullying a company, it has to go to the U.S. Government and deal with it in a diplomatic manner. And in a sense, it can reduce the transaction cost for an individual company, because it can say to them, much like companies have told us about the Foreign Corrupt Practices

Act, Hey, I cannot make this decision myself, I have to refer it to the U.S. Embassy or the U.S. Government entity within the Act.

Now, that is, to our knowledge, a way to address the issue. And, yes, there may be certain downsides to it, but instead of dismissing it as saying it is a conflict of laws or some other problem, I would challenge companies to come up with an effective alternative that meets the same objectives and propose it as legislation, rather than only looking at what the negatives of existing proposals are. I mean, we are more than happy to work with companies to think about that, but we think it needs to be there, because we need to change the dynamics. Because as long as the dynamic is a company having to deal with a Government about a repressive request, with no backstop, whether it is the U.S. Government or anything else, we are going to have this dynamic endlessly. So we need to change the rules in some way.

Chairman DURBIN. So, Ms. Wong, does that create a Catch- 22 for your company if they comply with the Chinese standards in censorship and there is a law in the United States which says that is a criminal act? How do you deal with that?

Ms. WONG. There would absolutely be a tension, and we have worked through that not just with China, but with many other countries around the world that assert their jurisdiction on the same areas.

Having said that, Mr. Chairman—and I am glad you raised it, because we have talking about it at our company, at our senior executive level, over the last several weeks—we would support legislation in this area because we do feel like it is the thing that will bring all the companies to the same place. It may be the most effective way to deal with the other countries.

Chairman DURBIN. So let me ask two wrap-up questions here of things that still I have a question in my mind that you testified to. Reporters Without Borders notes that Google is financing Baidu, the Chinese company that is a market leader in search engines. And you are saying that is not true.

Ms. WONG. We are not investors in Baidu.

Chairman DURBIN. OK. And, second, when it came to the code of conduct, as I understand it, Yahoo! said they would sign onto the code as is, and I think your statement was that you supported external audits. So would you accept the code of conduct as it currently is written?

Ms. WONG. We have put another proposal on the table. It involves external audits. I think that that is what we are currently working with the human rights groups on the nature of those audits, what is measured, how it is measured, who does the measuring. But we are confident that that will get finalized. We are optimistic it will get finalized.

Chairman DURBIN. And you can be confident that we are going to be watching you to make sure it does get finalized. After 18 months in this lightning fast communications world that we live in, what is slowing this down? Please, I hope that everyone will work in good faith to complete it.

Thank you for this fascinating and interesting panel, and the very expert testimony we received today. As I said, the hearing

record is going to remain open for a week for additional materials from interested individuals and questions for the witnesses.

At the end of the day, I am going to be sitting down with Senator Brownback to—or, pardon me, Senator Coburn—and Senator Brownback, for that matter—to discuss whether we are going to introduce legislation similar to that pending in the House or craft our own along these lines. I really think this is a critical area that we need to address forthrightly and honestly.

I want to salute some unsung heroes on my staff: Joe Zogby, who inspired me to ask for this Subcommittee and has been my leader on so many of these issues; Talia Dubov; Jaideep Dargan; Reema Dodin; Corey Clyburn, a legal intern; and Heloisa Griggs. They have done an awful lot of work to make this hearing a success.

Thank you all for being here. There will be statements for the record from a number of organizations that will be entered without objection, and since there is no one here to object, so ordered. The Subcommittee stands adjourned.

[Whereupon, at 11:55 a.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

Questions for the Record for Mark Chandler, Cisco Systems, Inc.
Senate Judiciary Committee
Subcommittee on Human Rights and the Law

Senator Durbin Questions

1. You testified, "We support restrictions on the ability of companies to locate within an internet-restricting country electronic communications that include personally-identifiable information." Does Cisco support H.R. 275, the Global Online Freedom Act of 2007? Please explain.

A1. Cisco believes that the U.S. government has an important role to play in protecting and promoting freedom of electronic information abroad. To focus these efforts, Cisco supports establishing an Office of Global Internet Freedom at the U.S. Department of State and appointing a U.S. Ambassador at Large for Internet Freedom. We understand that many companies that provide direct internet services to consumers, which Cisco does not, are voluntarily taking the step described in the question.

2. You testified that "employees would customize [Cisco's] products in such a way as to undermine human rights would not be consistent with the code of conduct that we have."

a. How would such customization be inconsistent with Cisco's code of conduct?

A2a. Such customization would be inconsistent with Cisco's core principles, embodied in our basic human rights guidelines adopted in Cisco's Corporate Citizenship Report which guide the conduct of our employees. As stated in our Corporate Citizenship Report 2007, Cisco "support[s] the United Nations Universal Declaration of Human Rights" and, as outlined in our Code of Business Conduct and employee policies, we expect all our employees to "treat others equally and with respect and dignity."

Cisco has adopted the following two principles from the UN Global Compact, as stated in the Report:

> *"Principle 1: Businesses should support and respect the protection of internationally proclaimed human rights; and*
>
> *Principle 2: Businesses should make sure that they are not complicit in human rights abuses."*

The Report further makes clear that with regard to our products and the indirect customers of our products:

> *• Cisco does not customize, or develop specialized or unique filtering capabilities, in order to enable different political regimes to block access to information.*

45688.001

• With respect to operating functionality, Cisco sells the same equipment in China as it sells worldwide.
• Cisco is not a service or content provider or network manager.
• Cisco has no access to information about individual users of the Internet.

b. Please provide a copy of this code of conduct and any other Cisco human rights guidelines or policies

A2b. See attachments.

3. At the hearing I asked you, "Does your company inform government clients, in writing or otherwise, that they will not assist in efforts toward censorship or repression?" You responded "our products do not do that." You also testified, "Cisco does not customize, or develop specialized or unique filtering capabilities, in order to enable different regimes to block access to information...The tools built into our products that enable site filtering are the same the world over, whether sold to governments, companies or network operators. The features in our equipment are 'off the shelf' and not altered in any way for any market or region."

a. Do you agree that Cisco's off-the-shelf products, which you testified "enable site filtering," can be used to enable different regimes to block access to information, even if they are not customized?

A3a. As I mentioned in my written testimony, the Internet can be and is disrupted by cyber attacks despite its redundant nature. Every major corporate and service provider network has experienced this. Attached to this letter is an article from the November 10 New York Times regarding the growing sophistication of attacks on public and private networks around the world.

Network management and security capabilities are essential to mitigate attacks and thus enable information flow. No network can be administered by our customers without the ability to manage and protect the information that flows through it. Without this capability, it would not be possible to operate the Internet, and the Internet would not exist as it does today.

Moreover, the technology that is used to manage and protect against hackers or viruses is the same generic technology used to filter or control Internet access by children, such as the parental control software that network operators are being urged to provide to all customers, or the illegal downloading of copyrighted material.

Network management software is a basic feature of Internet equipment -- Cisco's and our competitors' -- and fundamental to network functionality. Whether for security or the management of information, the technology is one and the same.

b. Do you stand by your testimony that "our products do not" assist in efforts toward censorship or repression in any circumstances?

45688.002

A3b. Our products are designed to expand the reach of the Internet and to ensure the stability, safety and availability of communications networks; without these network management and security capabilities, the Internet could not function. Our products are not designed for censorship or repression.

c. Let me ask you again, does Cisco inform its government clients, in writing or otherwise, that they will not assist in efforts toward censorship or repression?

A3c. As I note in my answer to 2a above, our Corporate Citizenship Report, which is publicly available, states our corporate policy on human rights. It specifically notes that our company does not develop specialized technology to enable regimes to block access to information, nor do we have access to individual user information of private internet users.

d. If not, will you consider adopting such a policy?

A3d: See answers to Questions 3(a) and 3(c) above.

Q4. You testified that the 2002 Cisco PowerPoint "Overview of the Public Security Sector" discussed at the hearing was the work of a low-level employee.

a. Did the reference in the PowerPoint to the Falun Gong as "evil" violate Cisco's code of conduct or any other Cisco policies?

A4a. The statement in question does not reflect Cisco's principles, policies or its sales and marketing strategy or approach. It is a quotation from a speech made by a Chinese government official in 2001. Reprinting a statement by a government official, even if the underlying sentiment is inconsistent with Cisco's policies, does not by itself violate those policies.

b. If the response to question 4(a) is no, will Cisco change its policies and procedures to make clear that such a reference is unacceptable.

A4b. See answer to Question 4(a), above.

c. If the response to question 4(a) is yes, was the employee who authored the PowerPoint disciplined?

A4c. See answer to Question 4(a), above.

d. According to Cisco's English translation, the PowerPoint described as one purpose of the Golden Shield project "Combat 'Falun Gong' evil religion and other hostiles." Is it therefore accurate to conclude that Cisco knew in

45688.003

2002 that one purpose of the Golden Shield was to combat Falun Gong and other religious or political dissidents?

A4d. The Chinese government's antipathy to Falun Gong has been long well-known. We regret that this quotation from a Chinese government official was reproduced in this 91-page presentation. The Golden Shield project, as we understand it, related generally to improved internal communication within the public safety departments. With respect to Cisco, Cisco sells the same off-the-shelf products in China as it does world-wide, consistent with U.S. law.

e. Has Cisco conducted an internal review to determine whether any documents similar to the 2002 PowerPoint exist?

A4e. No such review would be feasible or productive, given Cisco's size – 65,000 employees, operating in approximately 100 countries – and the fact that Cisco sells off-the-shelf products which are not customized. In no case does Cisco design products for repression or censorship. If contrary activity were to take place, Cisco would investigate any such report and take appropriate action.

f. If the response to question 4(e) is yes, please provide the results of this review, including any documents you discovered.

A4f. Not applicable.

g. If the response to question 4(e) is no, will Cisco conduct such a review and provide me with the results?

A4g. Literally tens or hundreds of thousands of documents globally describe the application of Cisco products to network implementation and modernization projects in the U.S. and around the world. We do not believe that such a massive review is feasible or productive, given that we sell standard equipment around the world which is not customized to enable different regimes to block access to information.

5.

a. What role did Cisco play in the development of the Chinese government's Golden Shield project?

A5a. To the best of my knowledge, Cisco did not play any role in the development of the Chinese government's Golden Shield project.

Cisco's standard switching and routing products have been acquired by various Chinese departments as part of their modernization programs, which could include, among others, the Golden Shield project. As noted above, Cisco does not customize its products to enable the blocking of information.

45688.004

b. Has Cisco ever described Golden Shield as one of its success stories?

A5b. Not to my knowledge.

6. Marketing

a. Can you assure me that Cisco does not in any circumstances market its product and/or services to government authorities in China or any other country on the basis of their usefulness in detecting, monitoring or censoring political dissent or expression that are protected under Article 19 of the International Covenant on Civil and Political Rights (ICCPR)?

A6a. As noted earlier, in a company with 65,000 employees located in approximately 100 countries, it is impossible to be certain whether any employee has ever violated any policy of the company, and this applies in this case as well. If such activities are detected, we will take appropriate action.

In any event, Cisco products are not designed or customized for the purpose of censorship or monitoring political dissent.

b. Can you be certain that no Cisco personnel market Cisco's products and services on this basis?

A6b. See answer to Question 6(a) above.

c. Will Cisco conduct a review to ensure that no Cisco personnel have engaged in this type of marketing?

A6c. See answer to Question 4(g) above.

d. What policies and procedures does Cisco have in place to ensure that Cisco personnel do not engage in this type of marketing?

A6d. See answers to Questions 2(a) and 6(a) above

e. Is this addressed in Cisco's code of conduct?

A6e. See answer to Question 2(a) above.

7. Services

a. Can you assure me that Cisco does not in any circumstances assist or advise government authorities in China or any other country in using your

45688.005

products for detecting, monitoring or censoring political dissent or expression that are protected under Article 19 of the ICCPR?

A7a. Cisco is not a traditional communications service provider or a web portal; rather we sell our products to these service providers. (Cisco's Webex subsidiary does provide an on-line conferencing and collaboration service that is used for web-based business communications). Since we do not tailor our products to allow for censorship, we believe our business in China and elsewhere is conducted fully in accord with our corporate principles, noted earlier.

All Cisco customers globally have access to Cisco training and support. We provide service and support, either directly or, in many cases, through systems integration partners for our equipment. Cisco service and post-sales support is generally designed to replace faulty or defective products, provide training for the proper operation of network hardware and ensure that networks are stable and available 24 hours a day, including protecting our customer's networks from hackers and malware.

b. Can you be certain that no Cisco personnel provide such assistance or advice?

A7b. See answer to Question 6(a) above.

c. Will Cisco conduct a review to ensure that no Cisco personnel have provided such assistance or advice?

A7c. See answer to Question 4(g) above.

d. What polices and procedures do you have in place to ensure that Cisco personnel do to [sic] not provide such assistance or advice?

A7d. See answers to Questions 2(a) and 6(a) above.

e. Is this addressed in Cisco's code of conduct?

A7e. See answer to Question 2(a) above.

8. What policies and procedures does Cisco have in place to ensure that your products and services are not used by government authorities in China or any other country to detect, monitor or censor political dissent or expression that are protected under Article 19 of the ICCPR?

A8. As stated above, Cisco has adopted the principles of the UN Global Compact, including that businesses should ensure that they are not complicit in human rights abuses and should support and respect the protection of internationally proclaimed human rights. Our products are off-the-shelf and are not customized to enable different

45688.006

political regimes to block access to information. Our products allow network administrators to manage and protect the information that flows through the network; without this capability, the Internet could not function.

9. You testified that "Cisco complies with all U.S. regulations informed by human rights concerns which control sale of our products."

a. Has Cisco ever refused a business opportunity to avoid complicity in human rights violations in a case where no law prohibited pursuing the opportunity?

A9a. Cisco is not complicit in human rights violations.

b. Would Cisco support changing U.S. regulations or laws to prohibit the export to China of networking equipment that can be used for censorship and surveillance?

A9b. Cisco will abide by all relevant U.S. statutes and regulations.

10. What products has Cisco sold to the Chinese government?

A10. For reasons of business confidentiality, Cisco cannot publicly disclose the details of customer purchases. Cisco would be pleased to discuss this with the Committee in confidence.

11.

a. Please describe "Policenet" in detail. What products does it include?

A11a. Cisco does not currently have, nor has it ever had, a product or solution referred to as "Policenet." It is our understanding that "Policenet" is a generic term used in many countries, including China, to refer to the concept of a networked police force.

b. What products and services does Policenet include?

A11b. Not applicable.

12. Would Cisco support an independent outside monitoring process, like the one that has been proposed for internet service providers, for companies that sell networking equipment to internet-restricting governments? Please explain.

A12. The business model for internet service providers and equipment vendors vary considerably, so I am not certain that what has been proposed would be appropriate. Cisco will abide by all relevant U.S. statutes and regulations.

13. Google's Nicole Wong testified, "We support the development of tools that are intended to get around censorship on the Internet. We do that in a couple of ways,

45688.007

both directly supporting developers in that area, and also providing a code base for building on top of that."

a. Does Cisco support developers of anti-censorship technology? Please provide examples.

A13a. I am not aware that we have been approached by any anti-censorship technology developers for assistance. To the extent that technologies are innovative and broaden the reach of the Internet, we would support such technologies.

b. You testified about "the respect I have for the efforts that [Shiyu Zhou] undertakes to allow access to information that censors would otherwise preclude access to." Will Cisco consider supporting the Global Internet Freedom Consortium?

A13b. The best way that Cisco can support the Global Internet Freedom Consortium is to continue to build our products to open, global standards and vigorously oppose attempts by some governments to balkanize the Internet by setting country-specific security requirements.

45688.008

Senator Coburn Questions

Q1. Please describe the efforts Cisco is making to ensure internet freedom to its customers around the world.

A1. As a global organization, Cisco has played a leading role in helping to make Internet technology ubiquitous. Doing this has enabled hundreds of millions of people in nearly every nation around the world to access information and ideas previously unavailable or inaccessible. We believe in maximum access to information and Cisco is proud of the role we have played in bringing the Internet to hundreds of millions of people around the world -- including by building open systems that facilitate efforts to overcome censorship.

Since entering the China market in 1994, Cisco along with other leading technology businesses have participated in helping increase the number of Chinese people who have access to the Internet – from 80,000 users in 1995 to over 253,000,000 in 2008.

Cisco remains committed to continuing to expand the reach of the Internet. To that end, Cisco invests billions annually in education, training and R&D to help bolster technology infrastructure and skills-development of people in emerging markets.

The Internet has been the greatest force in the world today for the dissemination of and access to information.

Q2. Is it Cisco's belief that its products are *not* being used by certain governments to further their censorship policies?

A2. Our products are not designed for censorship; they are designed to expand the reach of the Internet and to ensure the stability, safety and reliability of communications networks.

45688.009

APPENDIX

http://www.cisco.com/web/about/ac227/about_cisco_corp_citi_human_rights.html

Human Rights

Introduction

Cisco strives to treat employees, and the communities in which we serve, with respect and dignity.

A supporter of the United Nations Universal Declaration of Human Rights and Global Compact. Cisco's codes of conduct, employee policies and guidelines substantially incorporate laws and ethical principles including those pertaining to freedom of association, non-discrimination, privacy, collective bargaining, compulsory and child labor, immigration and wages and hours.

Consistent with Cisco's culture and applicable laws, employees are encouraged to:

promote a safe, healthy and supportive work environment where employees can contribute their skills, and

participate with local stakeholders in addressing community well-being, social and economic development and environmental preservation.

Employees shall respect the human rights and dignity of others as outlined in the Code of Business Conduct, employee policies, and guidelines or local laws applying and abiding within the scope of their individual roles and responsibilities to whichever sets higher standards.

Read more about Cisco's responsible management and CSR governance

Read more about Cisco's human rights policy and freedom of expression [TEXT FROM THIS LINK APPEARS BELOW]

Cisco engages with stakeholders in three primary ways: industry group stakeholder engagement, third-party facilitated individual interviews or convened groups, and ongoing conversations with established stakeholders.

Through these engagements, Cisco aims to gain perspective and insight regarding our corporate citizenship performance, specifically:

- To learn more about how Cisco's current corporate citizenship is perceived and where the company could be more transparent or change current practice
- To get forward-looking information from stakeholders with particular subject-matter expertise, industry knowledge, or insight into our lines of business and specified growth areas
- To provide Cisco leadership with a chance to listen to different perspectives and

45688.010

build ongoing relationships with key influencers

The feedback from recent stakeholder engagements indicates that our stakeholders believe Cisco has made progress in areas of corporate social responsibility (CSR). Stakeholders view Cisco as a leader in CSR, as evidenced by our participation in the **Electronic Industry Code of Conduct (EICC)** and the Global e-Sustainability Initiative (GeSI), for example. In addition, stakeholders view Cisco as transparent, accessible, and a strong performer, and they feel our participation in external groups is broad-ranging.

For the future, our stakeholders look to Cisco to provide more nuanced data and metrics in support of our CSR activities, as well as to anticipate trends and continue to play a leadership role in addressing emerging CSR issues.

Identified Issues

In addition to asking for feedback on Cisco's CSR performance, we actively solicit feedback on important emerging issues. The following issues were identified as most pressing:

- Individual rights to privacy, and how Cisco's products and services fit into that debate
- Data security and the development of technology solutions to address security
- Internet censorship and freedom of expression
- Cisco's position on Internet neutrality
- Cisco's CSR and corporate governance, particularly our internal implementation of policies
- China's policies toward the Internet
- Information on the management systems in place to place to meet our CSR goals
- Incentives for employees (and executives in particular) to meet our CSR goals and targets
- Political contributions

Cisco's 2006 report addressed stakeholder concerns for net neutrality, human rights, and privacy. This year we will address questions related to our responsible risk management, the relationships within our value chain, and our investigation of concerns raised by stakeholders concerning human rights and freedom of expression, and accessibility of the Internet, particularly in China

Issues Spotlight: Human Rights, Freedom of Expression, and China

We maintain a specific corporate policy on human rights and other codes and policies addressing human rights for our employees and suppliers. With regard to our product and the indirect customers of our products:

- Cisco does not customize, or develop specialized or unique filtering capabilities, in order to enable different regimes to block access to information.
- Cisco sells the same equipment in China as it sells worldwide.
- Cisco is not a service or content provider or network manager.
- Cisco has no access to information about individual users of the Internet.

45688.011

HUMAN RIGHTS WATCH
1630 Connecticut Avenue, N.W.
Suite 500
Washington, DC 20009
Tel: 202-612-4321
Fax: 202-612-4333
Email: hrwdc@hrw.org

Kenneth Roth, *Executive Director*
Michele Alexander, *Development & Outreach Director*
Carroll Bogert, *Associate Director*
Barbara Guglielmo, *Finance & Administration Director*
Peggy Hicks, *Global Advocacy Director*
Iain Levine, *Program Director*
Dinah PoKempner, *General Counsel*
James Ross, *Senior Legal Advisor*
Joe Saunders, *Deputy Program Director*
Wilder Tayler, *Legal and Policy Director*

PROGRAM DIRECTORS
Brad Adams, *Asia*
Holly Cartner, *Europe & Central Asia*
Peter Takirambudde, *Africa*
José Miguel Vivanco, *Americas*
Sarah Leah Whitson, *Middle East & North Africa*
Jamie Fellner, *United States*
Joseph Amon, *HIV/AIDS*
Peter Bouckaert, *Emergencies*
Bruni Burres, *International Film Festival*
Richard Dicker, *International Justice*
Bill Frelick, *Refugee Policy*
Arvind Ganesan, *Business & Human Rights*
Steve Goose, *Arms*
LaShawn R. Jefferson, *Women's Rights*
Scott Long, *Lesbian, Gay, Bisexual & Transgender Rights*
Joanne Mariner, *Terrorism & Counterterrorism*
Lois Whitman, *Children's Rights*

ADVOCACY DIRECTORS
Steve Crawshaw, *United Nations*
Marlette Grange, *Geneva*
Marianne Heuwagen, *Berlin*
Lotte Leicht, *European Union*
Tom Malinowski, *Washington DC*
Tom Porteous, *London*

BOARD OF DIRECTORS
Jane Olson, *Chair*
Bruce J. Klatsky, *Vice-Chair*
Sid Sheinberg, *Vice-Chair*
John J. Studzinski, *Vice-Chair*
Omar Amanat
Lloyd Axworthy
David M. Brown
Jorge Castañeda
Tony Elliott
Michael G. Fisch
Michael E. Gellert
Richard J. Goldstone
Vartan Gregorian
James F. Hoge, Jr.
Wendy Keys
Robert Kissane
Joanne Leedom-Ackerman
Josh Mailman
Susan Manilow
Kati Marton
Linda Mason
Barry Meyer
Pat Mitchell
Joel Motley
Samuel K. Murumba
Catherine Powell
Sigrid Rausing
Victoria Riskin
Kevin P. Ryan
Darian W. Swig
John R. Taylor
Shibley Telhami

Robert L. Bernstein, *Founding Chair, (1979-1997)*
Jonathan F. Fenton, *Chair (1998-2003)*
Bruce Rabb, *Secretary*

The Honorable Thomas Coburn
172 Russell Senate Office Building
Washington, DC 20510

HUMAN RIGHTS WATCH

www.hrw.org

July 18, 2008

Dear Senator Coburn,

Thank you for your follow-up questions in regards to the May 20, 2008 hearing *Global Internet Freedom: Corporate Responsibility and the Rule of Law.* Our responses to those questions are provided below.

1. **Do you believe that American companies should do business in countries that censor the Internet?**

We believe that the Internet is a critical medium to open societies and facilitate the free flow of information that is crucial for increased respect for human rights. For those and other reasons, we believe that, because both US companies and other companies can be important actors in closed societies, provided they aggressively work to curtail censorship, such companies should do business in as many countries as possible. Rather than leave, they should do everything they can to ensure that their products and services are not limited by censorship or other threats to human rights.

Where censorship or protection of cyberdissidents is an issue, we believe that companies should institute safeguards to minimize, if not eliminate, censorship. Those safeguards should include voluntary measures such as those discussed in the May 20, 2008 hearing. In order to further reduce censorship and to protect cyberdissidents, we also support regulatory measures such as those proposed in the Global Online Freedom Act, particularly in situations or in countries where companies are unwilling or unable to implement those protections themselves.

2. **What is the experience of other non-internet companies doing business in China? In other words, certain industries like book publishers or movie producers must also comply with local censorship laws. Are they under as much pressure as these internet companies to defy authority and promote the free flow of information?**

Our understanding is that book publishers have faced similar pressure to self-censor their products and regularly do so. For example, Harper Collins dropped the former British High Commissioner of Hong Kong, Chris Patten's, book in order to avoid offending the Chinese government. When the current head of Harper Collins was asked about censorship in China on the BBC in 2006, she said that she believed one had to respect different

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00051 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.012

"cultural sensitivities." In reference to Patten's book, she said, "you don't criticize Mickey if you work at Disneyland." Similarly, sections of former president Bill Clinton's memoirs were excised for distribution in China. We have no information to suggest that such companies are trying to combat such censorship.

3. **I have learned in preparing for this hearing that countries like Canada, France, Germany, and other surprising places require some kind of internet censorship. What is your position on those countries? Is any amount of censorship acceptable?**

We understand that, for numerous political, social, and historical reasons, there are restrictions to certain types of speech in European and other countries. We are sensitive to issues surrounding Nazi propaganda in Germany, "Hate Speech", and other issues where governments may try to restrict speech.

However, the right to freedom of expression is a fundamental one and, because it is essential for holding governments accountable to the public, it is necessary in order to protect the exercise of all other human rights in democratic societies. Freedom of expression is particularly necessary with respect to provocative or offensive speech. Once governmental censorship is permitted in such cases, the temptation is enormous for government officials to find speech that is critical of them to be unduly provocative or offensive as well. Taboos often mask matters of considerable public concern that are best addressed through honest and unfettered debate among those holding diverse points of view. Thus, the freedom to express even controversial points of view is important in order for societies to address key political, social, and cultural issues. Although international human rights law does impose certain limits on the right to freedom of expression, the important functions served by that right require interpreting those limitations narrowly. Freedom of expression may be limited to protect public safety and the rights of others, but such limitations must be strictly "necessary" in a democratic society. Banning provocative speech that does not imminently incite people to unlawful acts of discrimination, hostility or violence, rarely meets that test.

Laws that are intended to restrict speech can disproportionately restrict the protected right to freedom of expression. We are mindful that there are different perspectives on what is permissible and prohibited speech, but we base our position on a strong commitment to freedom of expression as a core principle of human rights and on our conviction that objectionable speech is best met with contrary speech, not censorship. We also believe that governments can best counter offensive speech by fulfilling their obligation to take positive measures to protect vulnerable groups, making clear that they reject all forms of discrimination, and ensuring that all groups have the right to present their views and counter those that they disagree with or find offensive.

4. **As you know, in 2005, Yahoo! gave up a majority stake of its China service to a Chinese company, Alibaba, thus ceding control of its daily operations to that entity. What are your thoughts on this sale, especially with respect to how it did or did not affect Yahoo's human rights responsibilities in China? Do you see this sale as a trend for American internet companies doing business with repressive regimes? Do you view this as a good or bad thing?**

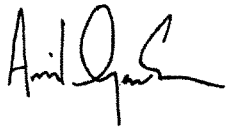
45688.013

We do not have any information to suggest that Yahoo sold its stake to Alibaba primarily to avoid its human rights responsibilities or to avoid liability that might stem from ownership in that company. We were disappointed with Yahoo's subsequent assertions that they could not control the actions of their subsidiary with respect to cases like that of Shi Tao because of their minority ownership in the company. In that respect, it did have a negative impact on human rights and on Yahoo's reputation. This business relationship also makes it more difficult for companies who want to protect human rights to enforce their standards in repressive countries or with certain business partners.

We have no information suggesting that such sales are a trend, but we are troubled by the possibility that companies might sell controlling interest to avoid human rights responsibilities. We do feel that there are some ways to address this problem. A voluntary measure should include a provision that companies cannot cede controlling interests in business ventures for the purpose of avoiding their human rights obligations. In order to minimize the possibility of human rights abuses occurring even when a company does not have full ownership of a business venture, legislation could include provisions that ensure that human rights obligations also apply to certain subsidiaries or other business ventures.

Thank you again for the opportunity to speak on this matter and please let me know if there is any more information you might require.

Sincerely,



Arvind Ganesan
Director
Business and Human Rights Program
Human Rights Watch

45688.014

Senator Richard J. Durbin
"Global Internet Freedom: Corporate Responsibility and the Rule of Law"
Senate Judiciary Committee
Subcommittee on Human Rights and the Law
Questions for the Record for Michael Samway, Yahoo!

1. **Does Yahoo! support H.R. 275, the Global Online Freedom Act of 2007? Please explain.**

   Yahoo! supports the objectives of GOFA and, in particular, the formalization of the Office of Global Internet Freedom. GOFA properly recognizes the leadership role the U.S. government must play in persuading foreign governments to respect more fully the online free expression and privacy rights of their own citizens. Yahoo! supports strengthening the U.S. government's ability to combat online censorship and the establishment of the Office of Global Internet Freedom to coordinate inter-agency efforts to promote Internet freedom – making permanent the Global Internet Freedom Taskforce with which Yahoo! has worked closely since it was created in 2006.

   We have worked with key GOFA stakeholders in Congress to find a path to achieve the goals of GOFA without instituting provisions that would have the practical effect of precluding engagement and preventing companies from bringing the transformative technologies of the Internet to people in certain areas of the world. Yahoo! does not believe that legislation should – in effect – bar companies from doing business in countries like China. While perhaps unintentionally, the minimum standards in the bill that prohibit U.S. businesses from complying with locally binding lawful orders would put companies and their local operations in the untenable position of having to choose to violate local law or violate U.S. law. This would likely mean that companies would have no choice but to cease doing business in countries like China. As a result, we have urged Congress to modify the current language to make it clear that companies would not be put in this unsustainable position.

2. **At the hearing, you testified, "We support backstop legislation, something that protects U.S. companies, but not legislation that puts us in the untenable position of having to choose to violate a local law or choose to violate U.S. law."**

   a. **Please elaborate on the nature of legislation that Yahoo! would support.**

   b. **Would such legislation ensure that American internet companies operating in internet- restricting countries protect user privacy and freedom of expression?**

   As indicated above, Yahoo! supports strengthening the U.S. government's ability to combat online censorship and the establishment of the Office of Global Internet Freedom to coordinate inter-agency efforts to promote Internet freedom – making permanent the Global Internet Freedom Taskforce with which Yahoo! has worked closely since it was created in 2006.

45688.015

Yahoo! does not believe that legislation should – in effect – bar companies from doing business in countries like China by, for example, prohibiting U.S. businesses from complying with locally binding lawful orders and putting companies in the untenable position of violating local law or violating U.S. law. This would likely mean that companies would have no choice but to cease doing business in countries like China.

Yahoo! has been working closely for the past two years with industry partners, academics, human rights organizations, socially responsible investors, and others to develop a global code of conduct that will guide technology companies operating in challenging markets. As we noted in our letter to your office on August 1, 2008, we have reached agreement in principle on the core components of this code, and we expect to formally launch the code this fall. Given the speed of change in technology and companies' ability to reach users around the globe, Yahoo! believes that a voluntary code can be nimble and ultimately most effective in protecting individual rights. At the same time, while the code will be global in nature and has participants from around the world, we also believe Congress can play an important role in promoting support for and adherence to the code of conduct.

3. **Cisco's Mark Chandler testified, "We support restrictions on the ability of companies to locate within an internet-restricting country electronic communications that include personally-identifiable information." Does [Yahoo!] support such restrictions?**

Yahoo! believes global engagement serves the interests of access to information and freedom of expression. Yahoo! also recognizes its responsibility to anticipate and mitigate human rights risks in making business decisions. Accordingly, Yahoo! has developed a human rights impact assessment process by which Yahoo! assesses the human rights conditions in challenging countries as well as the legal requirements and restrictions for operating in such countries. This in-depth review allows Yahoo! to plan and structure its service offerings — as well as its legal and operational structure — to limit the potential risks to human rights, while providing services that can advance the exchange of information and communication and have a positive effect on the lives of citizens in those countries.

One important factor in a human rights risk assessment is considering the implications of data location and data access as well as the impact on the rights of both users and local employees. We focus closely on these critical questions in designing risk mitigation strategies for our products and operations in challenging markets. And while we believe it is essential to limit risks of compelled data disclosure, data access, and data seizure, we also know foreign governments have many sources of leverage over companies doing business in their countries. Those sources of leverage include assertion of jurisdiction, revocation of licenses, blocking of services, threats of civil or criminal sanctions against local employees, physical seizure of data, or physical access to data.

We have also learned that it will not necessarily always be clear what will constitute personally identifiable information in this complex and dynamic industry. Declaring unequivocal support for a categorical restriction in this technical area may be overbroad and fail to account fully for the technical realities of personal data. As a result, such a

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00055 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.016

categorical restriction may prevent companies from bringing the transformative technologies of the Internet to people in certain areas of the world and could also inadvertently limit the risk mitigation strategies companies could adopt in any effort to limit human rights risks.

4. **Google's Nicole Wong testified that Google "would support an external audit" of their operations.**

   a. **Would Yahoo! support an external audit? If so, please describe the nature of the audit to which you would agree.**

   b. **Would you support an audit which is conducted by a monitor who is independently selected?**

   c. **Would such a monitor be permitted to assess whether Google has policies designed to protect freedom of expression and user privacy, how those policies are implemented, and whether the policies actually protect user privacy and freedom of expression?**

   d. **Would such a monitor have access to all relevant information, not just information Yahoo! chose to provide to him or her?**

As we noted in our letter to your office on August 1, 2008, as part of our participation in the multi-stakeholder process to create an industry code of conduct, Yahoo! does support independent external assessment of participating companies to review and evaluate their implementation of, and compliance with, the principles the group has set-out on free expression and privacy. External assessors would meet established competency and independence criteria. Companies would prepare reports for the independent assessors to review, and the assessors would have access to other relevant company data. Access would be subject to reasonable limitations such as attorney-client privilege, trade secrets or other disclosures restricted by law, and each company would identify with practicable specificity the reasons requiring the limitation. As we noted in the above-referenced letter, we believe a key component of the upcoming industry code of conduct must be a governance, accountability and learning framework founded on the notion that an organizational and multi-stakeholder governance structure is required to support the principles of free expression and privacy and that participating companies should be accountable for their role in the implementation of these principles through a system of independent assessment.

5. **What policies or practices does Yahoo! have in place to protect user privacy and freedom of expression in foreign countries?**

With respect to the freedom of expression and privacy of users of local services offered by Yahoo! subsidiaries, as explained more fully in response to questions 7 and 8 below, Yahoo! Inc.'s policy is that Yahoo! companies and operations around the world comply with lawful demands from governments — whether demands for content filtering, content removal or law enforcement demands for user data — from the countries in which they operate, consistent with local legal requirements, and do not comply with

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00056 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.017

requests believed to be outside the bounds of applicable law. Yahoo! Inc.'s policy is for its family of companies to challenge requests believed to be beyond the scope of what is required under local law, and Yahoo! Inc.'s policy is that each of the Yahoo! family of companies will comply with demands only where a government abides by the legal processes required by that country's laws. When a lawful demand is issued consistent with local legal requirements, and it is clear that compliance is compulsory under the local law, a Yahoo! company may be compelled to comply. This is what is expected in the United States from companies doing business here, and it is what foreign governments require of companies operating in their jurisdictions. This basic policy — that local operations or subsidiaries comply with legal demands from local jurisdictions and refuse to comply with requests outside the authority of the requesting entity — is consistent throughout the Yahoo! family of companies worldwide.

6. Please provide a list of all the localized services that Yahoo! offers.

Yahoo! Inc. provides services in the United States. Insofar as Yahoo! Inc. services are generally available on the Internet, services offered by Yahoo! Inc. may be accessed anywhere in the world the Internet is available.

Yahoo! has a local presence (meaning employees or representatives and a locally targeted Yahoo! website) in the following countries through a subsidiary, joint venture, investment, partnership, or other interest:

Argentina	Germany	Mexico
Australia	Hong Kong	New Zealand
Brazil	India	Singapore
Canada	Ireland	Spain
China	Italy	Taiwan
France	Japan	United Kingdom
	Republic of Korea	

For the following countries, Yahoo! operates a locally targeted website principally operated or hosted from another jurisdiction:

Austria	Malaysia	Sweden
Chile	Netherlands	Switzerland*
Colombia	Norway	Thailand
Denmark	Peru	Turkey
Finland	Philippines	Venezuela
Greece	Poland	Vietnam
Indonesia	Russia	

* The Yahoo! Swiss website is currently hosted from Germany and linked to the Yahoo! Germany website. It is important to note, however, that Yahoo! recently opened corporate offices in Switzerland and the situation there may change over time.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00057 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.018

7.

a. What process does Yahoo! follow when you receive a request for personally-identifiable user information from a foreign government?

b. Do you make an independent assessment of whether such a request complies with the law of the foreign country making the request?

c. In what circumstances would you decline or challenge in court such a request?

d. Have you ever declined or challenged such a request? Please explain.

e. Who at Yahoo! is ultimately responsible for authorizing the disclosure of personally-identifiable user information?

As part of Yahoo!'s commitment to protecting users' privacy and maintaining their trust, while at the same time fulfilling our public responsibility and legal obligations to respond to demands from authorized government entities in their efforts to enforce laws and protect public safety, Yahoo! has adopted principles to guide our practices in each jurisdiction where Yahoo! responds to government demands for user data.

Our key principles begin with Yahoo!'s commitment to ensuring that government demands for user data receive serious and careful attention. Additionally, Yahoo! Inc.'s policy is for its local services to disclose user data to governments only if disclosure is pursuant to valid legal process and consistent with applicable law. Yahoo! may also disclose information in certain exceptional circumstances, such as to prevent death or serious physical injury or reporting incidents where Yahoo! or its users have been victims of fraud or other crimes. Under Yahoo! Inc.'s policy, the local Yahoo! service should comply with a government demand only if the demand comes from an authorized government official or entity with the necessary jurisdictional authority over users of that service. Yahoo! Inc.'s policy is for its local service to carefully review each demand for user data and endeavor to narrowly interpret demands to limit the data disclosed to only that which is required to comply with the demand. Yahoo! Inc.'s policy contemplates the consideration of appropriate options when faced with a government demand for user data that raises privacy or human rights concerns, including the escalation of the demand, to the extent permitted by applicable law, for a legal review and, as appropriate, a human rights review. The options for responding to what appears to be an improper demand include partial compliance in a manner consistent with law, refusal to comply unless defects to the demand can be remedied, or challenges to such demands before an appropriate court.

8.

a. For which localized services do you censor political or religious content?

b. For each of these localized services, how do you determine what to censor?

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00058 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.019

c. **What process does Yahoo! follow when you receive a request from a foreign government to censor political or religious content?**

d. **Do you make an independent assessment of whether such a request complies with the law of the foreign country making the request?**

e. **In what circumstances would you decline or challenge in court such a request?**

f. **Have you ever declined or challenged such a request? Please explain.**

g. **Who at Yahoo! is ultimately responsible for authorizing the censorship of political or religious content?**

Yahoo! and its industry peers face limitations on content in many markets, ranging from prohibitions on certain forms of speech in France and Germany and hate speech regulations in many jurisdictions including the United States to search filtering requirements regarding political content applicable to Yahoo!'s former subsidiary in China. As with law enforcement demands for user data, Yahoo!'s policy is that its local service complies with the local law applicable to the local service's operations. Under this policy, Yahoo!'s local subsidiary or local operating entity should review any demand for content limitation or demand to remove content and assess that demand under applicable local law. Yahoo! Inc.'s policy is to construe such requests as narrowly as possible consistent with local law and challenge requests it believes are beyond the scope of what is required under local law. Also, Yahoo! Inc.'s policy is that each of the Yahoo! family of companies can and does require that a country abide by its own legal processes.

Employees of the legal department of the relevant subsidiary or operating unit are responsible for implementing this policy and escalating non-typical cases to Yahoo! Inc. Yahoo! has launched a formal Business & Human Rights Program to guide company decision-making in the areas where Yahoo!'s products and operations come into contact with international issues of free expression and privacy.

In one well-known legal case, Yahoo! Inc., which operates the service at www.yahoo.com, was ordered by a French court to remove content that was protected political speech under U.S. law. The content in question was available to users in France due to the nature of the global Internet, but was deemed illegal by French authorities. In that case, Yahoo! Inc. noted in the ensuing lawsuit that its French subsidiary, Yahoo! France, was in compliance with French law and did not display such content, but that Yahoo! Inc. was a U.S. company in compliance with U.S. laws. Yahoo! Inc. filed for declaratory relief action in U.S. district court asking it to find the judgment unenforceable because of inconsistency with the First Amendment. (Ultimately the Ninth Circuit Court of Appeals, ruling only on the jurisdiction question, ruled Yahoo! Inc. would have to wait until enforcement was actually filed in the United States against Yahoo! Inc.).

9. **At the hearing, I asked about the Chinese government's attempts to suppress information about the SARS epidemic. In the event of another public health emergency in a country that suppresses such information, how would Yahoo!**

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00059 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.020

respond to a censorship or takedown request regarding information about that health threat?

Yahoo! seeks to afford all of its users access to unfiltered information regarding public health issues through Yahoo!'s websites, and Yahoo! Inc., whose service is found at www.yahoo.com and is available across the globe, would not filter such content unless required to do so under United States law. As noted above, Yahoo! Inc.'s policies regarding content filtering limits filtering to the narrowest possible extent required by local law for the respective local services.

Where Yahoo! Inc. has a local subsidiary or operations subject to local law, those services must comply with applicable local law. In the hypothetical case posed, where Yahoo! Inc. had operational control over the local subsidiary, Yahoo! Inc.'s policy would require the local operation to confirm the lawfulness of the demand, interpret the government demand as narrowly as possible, and consider escalating the issue or challenging the demand if it were believed to be invalid.

10. **Human Rights Watch's Arvind Ganesan testified, "disclosing censorship is not enough, but actually actively trying to reduce it to where your minimum level is whatever the government says it is." Please describe what Yahoo! has done to reduce censorship to the minimum level.**

In February 2006, Yahoo! made the following four public commitments:

First, Collective Action. Yahoo! will continue to work with industry, government, academia and non-governmental organizations to explore policies to guide industry practices in countries where content is treated more restrictively than that in the United States and to promote the principles of freedom of speech and expression.

Second, Compliance Practices. Yahoo! continues to employ rigorous protections under applicable laws in response to government requests for information, maintaining its commitment to user privacy and compliance with the law.

Third, Information Restrictions. Where a government requests that Yahoo! restrict search results, Yahoo! does so if required by applicable law and only in a way that impacts the results as narrowly as possible. If Yahoo! is required to restrict search results, we strive to achieve maximum transparency to the user.

And fourth, Government Engagement. Yahoo! continues to engage actively in ongoing policy dialogue with governments around the world with respect to the nature of the Internet and the free flow of information.

Since 2006, we have acted on these commitments. Yahoo! has been working closely for the last two years with industry partners, academics, human rights organizations, socially responsible investors, and others to develop a global code of conduct that will guide technology companies operating in challenging markets. As we noted in our letter to your office on August 1, 2008, we expect to launch this initiative in the fall.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00060 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.021

We have also worked with industry peers and policy groups, as well as with the State Department's Global Internet Freedom Taskforce, to explore further ways to promote internet freedom globally.

With respect to China, China Yahoo! now provides notice on its search pages indicating results may have been narrowed or omitted due to legal restrictions. Users registering for a China Yahoo! e-mail account are alerted that the service is provided subject to Chinese law.

11. **Global Internet Freedom Consortium's Shiyu Zhou testified, "for companies like Google and Yahoo!, their self-censorship in China I would say is more damaging than other kinds of censorship, because for Chinese people in such a closed society, they take Google and Yahoo! as role models of freedom of information. When they look on the websites and they find the information, they believe it is factual and it is true." Do you agree?**

Yahoo! was founded on the principle that promoting access to information can fundamentally improve people's lives and enhance their relationship with the world around them. We believe that such access will ultimately help advance freedom of expression and, more broadly, individual rights worldwide. We believe the policies and practices of the companies in our industry should promote open access to the Internet while working on multiple fronts to prevent restrictions on this access. Yahoo! is also committed to user transparency. For that reason, we encouraged Alibaba to include a search notice, and China Yahoo! now includes a notice on its search pages indicating that results may have been narrowed or omitted due to legal restrictions.

12. **Please provide a copy of any human rights guidelines, policies, and training that Yahoo! has in place.**

Yahoo! has the utmost commitment to user privacy and free expression, and has endeavored to incorporate that commitment into its policies and practices, as outlined above. Yahoo! has made reaching agreement on an industry code of conduct a priority in its intensive engagement with a diverse group of interested parties — which include, in addition to Yahoo!, representatives of human rights organizations, policy groups, other companies, socially responsible investors, and academics. Moreover, even as these negotiations were on-going, Yahoo! independently undertook a number of affirmative steps to ensure that it remains an industry leader on these issues, including undertaking a comprehensive review of its law enforcement compliance policies globally, initiating substantial changes in its decision-making process in order to more fully ensure that human rights concerns are incorporated into the business review process, and continuing to invest in research into human rights and technology issues through Yahoo! fellowships at Georgetown University and Stanford University.

On May 7, 2008, Yahoo! publicly launched its Business & Human Rights Program (http://ycorpblog.com/2008/05/07/business-and-human-rights/). Through this program, Yahoo! has created a dedicated team to guide company decision-making on human rights

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00061 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.022

issues, create escalation paths for issues, conduct human rights impact assessments, engage with internal and external stakeholders, and create an accountability framework.

Yahoo! also continues to work with noted Chinese dissident and human rights activist Harry Wu and his Laogai Research Foundation in connection with the Yahoo! Human Rights Fund, which was created to provide humanitarian and legal support to political dissidents imprisoned for expressing their views online, as well as providing support to their families.

Because Yahoo!'s internal policies and procedures relating to these issues contain confidential, proprietary, and privileged information, and given the sensitive nature of, and legal restrictions applicable to Yahoo!'s law enforcement compliance efforts, Yahoo! is not in a position to provide the requested materials. Yahoo! is committed to working with your office on these important issues, and we have engaged with your staff regarding many of the details of these policies. We would be pleased to meet privately with you or the Committee staff to discuss Yahoo!'s policies, procedures, or practices in a way that does not breach confidentiality or privilege, and does not reveal sensitive or restricted law enforcement compliance information improperly.

13. **You testified that Yahoo! "currently conduct[s] - and I think we may be the only company to publicly announce and commit to this - a human rights impact assessment before entering any market." Please provide more information about these impact assessments, including for what new markets you have conducted such assessments, how you conduct such assessments, and how the results of such assessments have affected whether to enter a new market.**

Yahoo! Inc.'s experience in China has resulted in significant change within the Yahoo! family of companies, and the recent experience with preparing to expand service offerings in Vietnam is a good example. For Vietnam, in addition to the usual business review of the market, Yahoo! Inc. developed a human rights impact assessment, in which Yahoo! Inc. assessed the human rights conditions in Vietnam (including reports of the leading human rights organizations, academics, and the U.S. government). The company also consulted human rights experts and worked with the State Department and the U.S. Embassy and Consulate in Vietnam. The company dispatched a team to meet with U.S. officials in Vietnam regarding the challenges and opportunities, and it assessed the regulatory requirements and restrictions for operating in the country. This in-depth review has allowed Yahoo! to plan and structure our service offerings — including the legal and operational structure — in a way that attempts to limit the potential risks to human rights, while providing services that can advance the exchange of information and communication and have a positive effect on the lives of citizens there. The human rights review process associated with this business decision and the steps taken to limit potential human rights risks reflects Yahoo!'s renewed commitment to remaining a responsible actor in this area. Yahoo! has formalized the human rights impact assessment process and any such assessments will be conducted on an going-forward basis for new products or new markets that raise substantial human rights challenges.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00062 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.023

14. At the 2006 HIRC hearing, Yahoo!'s Michael Callahan testified, "We do not have day-to-day control over Yahoo! China, but as a large equity investor, we have made clear our desire that Alibaba continue to apply rigorous standards in response to government demands for information about its users. I have personally discussed our views with senior management of Alibaba, as have other senior executives of Yahoo!" You testified, "With respect to Alibaba, we also have exerted our influence with respect to the free flow of information in China." Please explain how Yahoo! has exerted its influence with Alibaba and provide specific examples of how that has changed Alibaba's policies and practices regarding user privacy and freedom of expression.

As one of four directors on Alibaba's board of directors, our Chief Executive Office Jerry Yang has had discussions with senior management of Alibaba to impress upon them the importance of these issues to Yahoo! Inc. Other Yahoo! Inc. employees, including Mr. Callahan and other members of the Yahoo! legal team, have also had discussions with Alibaba and Yahoo! China regarding these issues. Subsequent to these discussions, Alibaba's China Yahoo! service has taken specific steps to institute more transparent disclosure notices as part of its operations. First, China Yahoo! now provides notice on its search pages indicating that results may have been narrowed or omitted due to legal restrictions. Second, users registering for a China Yahoo! e-mail account are alerted that the service is provided subject to Chinese law.

Representatives of Yahoo! Inc. have also spoken both with officials at the State Department and directly with Chinese officials regarding the company's concerns about these matters, and particularly the Shi Tao case. Mr. Yang has met with State Department officials and has personally asked Secretary Rice to raise this issue with the Chinese government, which Yahoo! understand she did earlier this year in Beijing. Yahoo! Inc. encourages continued government-to-government efforts by the U.S. Congress and Executive Branch to effect changes in China's law enforcement practices.

15. Google's Nicole Wong testified, "We support the development of tools that are intended to get around censorship on the Internet. We do that in a couple of ways, both directly supporting developers in that area, and also providing a code base for building on top of that."

h. Does Yahoo! support developers of anti-censorship technology? Please provide examples.

i. You testified that "we are going to explore Dr. Zhou's organization and the technology offered." Have you followed up on this commitment? Please explain.

As a technology company, Yahoo! recognizes that technology can be part of the solution in combating censorship and promoting Internet freedom. Our team has met with Dr. Zhou in person to learn more about his organization and the role of technology in combating restrictions on the free flow of information online. We also agreed with Dr. Zhou to have further discussions between his technical teams and our own. While

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00063 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.024

technology is an important component of the solution, we also believe this issue should be addressed at a human level through the various tools of diplomacy and continued efforts of the U.S. government, including at the State Department. We believe the U.S. government has the most leverage to modify the practices of repressive regimes. Recognizing the responsibility of corporations, Yahoo! has also sought to build our internal capacity to make responsible corporate decisions on human rights issues.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00064 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.025

Senator Tom Coburn
"Global Internet Freedom: Corporate Responsibility and the Rule of Law"
Senate Judiciary Committee
Subcommittee on Human Rights and the Law
Questions for the Record for Michael Samway, Yahoo!

1) **If the Chinese government approached Yahoo! today with the same document it used to solicit the information that led to Shi Tao's imprisonment, how would the company handle the situation differently?**

We deeply regret that information demanded of Yahoo! China by Chinese authorities was used to prosecute citizens expressing their political views online. Today, Yahoo! Inc. has a non-controlling investment in the Chinese company Alibaba, which in turn runs China Yahoo!. Yahoo! Inc. does not manage the China Yahoo! business or make decisions regarding China Yahoo!/Alibaba's specific responses to Chinese government demands made under Chinese law. We will, however, continue to exert what influence we can on Alibaba with respect to privacy and data disclosure issues as well as free expression and political speech issues.

Any company's operations in foreign markets must comply with the local laws where that company is doing business – particularly with regard to law enforcement demands – just as foreign companies operating in the United States must abide by our laws. In those markets where governments limit freedom of expression and fail to sufficiently respect online personal privacy, companies contend with complex questions of local sovereignty and jurisdiction balanced against unique opportunities to offer innovative information and communications tools to ordinary citizens in that market.

In part as a result of our experiences in China, Yahoo! has developed a human rights impact assessment process by which Yahoo! assesses the human rights conditions in challenging countries as well as the legal requirements and restrictions for operating in such countries. This in-depth review allows Yahoo! to plan and structure its service offerings — as well as its legal and operational structure — to limit the potential risks to human rights, while providing services that can advance the exchange of information and communication and have a positive effect on the lives of citizens in those countries.

Yahoo! has worked closely with industry partners, human rights groups, socially responsible investors, and academics on a global framework for technology companies operating in countries that unfairly restrict free expression and privacy. As we noted in our letter to your office on August 1, 2008, we expect to launch this initiative in the fall. Yahoo! has also encouraged a more active role by the U.S. government on these issues, given the government's diplomatic and economic leverage.

2) **How much of Yahoo!'s decision to sell its China division to Alibaba was based on concern over its responsibility for the human rights issues that were coming to light around the same time? At the time of the sale, did Yahoo! know anything about its involvement in the case of Shi Tao?**

45688.026

Yahoo!'s decision to sell its China division to Alibaba was unrelated to the Shi Tao case. Yahoo! began negotiating the sale of its China operations to Alibaba in early to mid 2005 and signed the deal with Alibaba in August 2005. Our team learned about Shi Tao's identity and imprisonment, and connection to Yahoo!, when it was reported publicly in September 2005. The sale and our ongoing minority stake in Alibaba is similar to Yahoo's investment structures in other countries, and reflected our approach to finding strong local management to run the business, as well as local engineering expertise to power the product efforts.

3) Does Yahoo! have any reservations about allowing its name to be associated with a Chinese company over which it does not have day-to-day control?

We deeply regret that information demanded of Yahoo! China by Chinese authorities was used to prosecute citizens expressing their political views online. We were a pioneer among American Internet companies, entering China around the time of normalization of trade relations by the U.S. Congress. We made a strategic business decision in 2005 to sell the Yahoo! operations in China to a Chinese company in order to grow the business in that important market more effectively. The sale included a license to Alibaba to use the Yahoo! name in China. We continue to believe engagement in markets overseas is important and that the Internet is a transformative medium that has the power to change the way ordinary citizens learn about their own communities and about the outside world as well as the way they communicate with one another. Nevertheless, we remain concerned about activities in China and anywhere in the world where citizens are punished for expressing their political views online. For this reason, we have continued to express concern to China Yahoo! about these issues and to try to exert influence upon China Yahoo! to inform users about such risks.

4) Has Yahoo!'s affiliation with Alibaba proven profitable for the company?

Our investment in Alibaba and other investments in Asia have been financially and strategically valuable to Yahoo! and its shareholders. We also recognize our obligation to be a good global corporate citizen. We take that obligation seriously and will continue to exert our influence on Alibaba with respect to privacy and data disclosure issues as well as free expression and political speech issues. We believe the best way to bring the power of the Internet to people around the world and to help promote meaningful and positive change is through global engagement and investment.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00066 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.027

Questions from Senator Dick Durbin

1. Does Google support H.R. 275, the Global Online Freedom Act of 2007? Please explain.

Google supports the Global Online Freedom Act because of the company's deep belief in and commitment to internet freedom, and we believe that the legislation can be improved to help ensure that people around the world have even greater access to as much information as possible. For example, we invite the Subcommittee to consider a legislative proposal made recently by the Center for Democracy and Technology that would help protect individuals' freedom of expression and privacy while not hindering the proliferation of free expression technologies throughout the world.

We also believe that the most effective aspect of GOFA would be to help ensure that the United States government engages in direct government-to-government discussions and robust international efforts to better ensure individuals' protection from government persecution and their right to free expression. Accordingly, we support initiatives to address online freedom of expression through international human rights and trade mechanisms.

Google's experience is that efforts to limit freedom of expression on the web exist in several nations around the world, and that the U.S. and other nations that cherish free expression are strongly positioned to fight these efforts to limit access to information on the Internet. As Nicole Wong testified at your Subcommittee's hearing on global internet freedom, we have recently seen several examples of censorship that pan several products and approximately 24 countries:

- ***YouTube***: Since 2007, our YouTube video sharing site has been blocked in at least 11 countries including China, Thailand, Turkey, Pakistan, Morocco, Brazil, Syria, Indonesia, Iran, Saudi Arabia, and Myanmar (Burma).

- ***Blogger and Blog*Spot***: In the last couple of years, we have received reports of our Blogger and Blog*Spot blogging sites 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.

Specifically, we believe that, as part of any legislation considered, Congress should take into account the following policy recommendations, which we presented at your Subcommittee's May 20 hearing on global internet freedom:

- ***Leverage international trade mechanisms***. The U.S. government should continue to urge governments around the world to recognize that information restrictions on the Internet have a trade dimension. We urge the U.S. government to continue to use trade agreements and other trade tools to promote the free flow of information on the Internet, and to seek binding commitments wherever possible.

- ***Promote the universal ratification of the International Covenant***. Not every country that has signed the International Covenant on Civil and Political Rights (ICCPR) has fully embraced its obligations by ratifying it. Approximately 30 countries are not parties to the agreement, including China, Cuba, and Saudi Arabia. We would strongly recommend that

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00067 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.028

the U.S. renew diplomatic efforts to encourage these countries to ratify the ICCPR, and to file separate declarations under the treaty to consent to the United Nations Human Rights Committee's jurisdiction over complaints by States against other States. We also believe that more governments – including the U.S. – should be encouraged to join the ICCPR's First Optional Protocol, which enables individuals to file complaints.

- ***Strengthen and enhance the State Department's Global Internet Freedom Taskforce.*** Much has been accomplished by the State Department's Global Internet Freedom Taskforce, but the initiative could be given increased prominence, authority, and funding. Among other things, the agenda could be given increased prominence and authority by, for example, appointing an Ambassador-at-Large for Information Freedom – a position similar to the Ambassador-at-Large for International Religious Freedom.

- ***Support increased focus by the U.N. Human Rights Committee on internet freedoms.*** In the area of internet censorship, the States Parties to the ICCPR could focus more attention on impediments to free expression online. For example, the Human Rights Committee could issue a general comment addressing relevant articles in the ICCPR and how they apply to internet restrictions.

- ***Ensure that countries that are parties to the Covenant submit human rights reports enabling international review.*** The ICCPR requires States Parties to submit periodic reports on compliance with their ICCPR obligations – generally every four years – to the U.N. Human Rights Committee, which conducts a detailed review and issues an assessment of treaty compliance. Many governments have not complied with this requirement, and the U.S. itself was out of compliance until it submitted a report in late 2005. The U.S., now having fully embraced its reporting obligations, should work to ensure that States Parties file their reports on compliance with the ICCPR in a timely fashion. This may need to involve offers of support for developing countries who are daunted by the effort involved in drafting the reports and submitting them for review, but we believe that this would be a worthwhile investment that would help protect human rights around the world.

- ***Strengthen individuals' ability to file complaints under the ICCPR.*** The ICCPR enables individuals to file complaints with the Human Rights Committee. We believe that the governments that promote free expression could provide funding and other support to non-governmental organizations and other groups to assist individuals in filing such complaints, as well as increasing awareness among relevant populations of their rights under the ICCPR. In addition, participating governments could, through the U.N., provide additional funding that would enable the Human Rights Committee to address more individual complaints in a timely way, as the Committee is now substantially underfunded.

- ***Shine more light on violations of freedom of expression.*** We believe that more attention focused on instances of internet censorship will result in greater accountability and transparency and ultimately less censorship by governments. For these reasons we would urge the U.S. government to promote enhanced monitoring of instances of internet censorship by governments.

- ***Promote free expression as part of foreign aid.*** We believe that the U.S. government could use foreign aid and other programs to better promote ICCPR compliance and free

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00068 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.029

expression on the Internet. For instance, the U.S. government could incorporate internet freedom of expression into support for and assessments of good governance. In a related area, Google has already urged officials at the Millennium Challenge Corporation to incorporate internet censorship in their criteria for measuring whether candidate countries have achieved expectations for democratic governance.

2. At the hearing, you testified, "we have been talking about it at our company at our senior executive level over the last several weeks - we would support legislation in this area because we do feel like it is the thing that will bring all the companies to the same place."

a. Please elaborate on the nature of legislation that Google would support.

We are supportive of GOFA and of the policy initiatives listed in response to question 1 above.

b. Would such legislation ensure that American internet companies operating in internet restricting countries protect user privacy and freedom of expression?

We believe that GOFA, along with the policy initiatives outlined in response to question 1 above, could help ensure the protection of user privacy and freedom of expression, especially if the legislation were improved to avoid impeding the spread of technologies around the world that promote free expression.

3. Cisco's Mark Chandler testified, "We support restrictions on the ability of companies to locate within are internet-restricting country electronic communications that include personally-identifiable information." Does Google support such restrictions?

Please see our answer to question 1 above.

4. You testified that Google "would support an external audit" of your operations.

a. Please elaborate on what sort of external audit you would support.

Google and other companies have joined human rights groups in support of the Global Network Initiative (GNI) which, in addition to establishing core principles for protecting freedom of expression and privacy around the world, includes an external audit for the companies. Having done our due diligence on the workability of the GNI principles, Google has committed to their implementation. Indeed, Google continues to adhere to the policies we ourselves announced in January 2006, committing the company to transparency about speech restrictions, and to carefully implemented protections for user data. We consult regularly with outside advisers to determine how to best respond to government requests that relate to freedom of expression or that involve our users' information. When we believe that doing so will help promote the cause of free expression, we publicize instances of government requests and our response to such requests.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00069 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.030

b. Would you support an audit which is conducted by a monitor who is independently selected?

In line with the Global Network Initiative principles, we support assessments by qualified outside experts that would be chosen based on close consultation with Google and the board of a proposed independent organization. As recognized in the Global Network Initiative, an effective audit in this area requires an auditor who has experience with business operations, human rights, and technology, and an appreciation for the complex technical and operational issues involved in implementing the principles

c. Would such a monitor be permitted to assess whether Google has policies designed to protect freedom of expression and user privacy, how those policies are implemented, and whether the policies actually protect user privacy and freedom of expression?

Please see our answer to question 4(a) above.

d. Would such a monitor have access to all relevant information, not just information Google chose to provide to him or her?

Please see our answer to question 4(a) above.

5. Regarding a code of conduct for internet companies, you testified that "the importance of having all of the companies and the addition of the human rights groups is not necessarily about looking about whether the companies are being held accountable to their processes." Who do you believe it is not necessarily important to hold accountable internet companies operating in internet-restricting countries?

The observation was made to highlight a single point: An effective front against internet censorship requires broad, global participation in the principles.

The original premise of establishing agreed-upon free expression and privacy principles was for companies and human rights groups to stand together and speak with one voice against oppressive governments, and to enlist the support of governments that respect and protect free expression in those efforts. The focus on monitoring specific processes of individual companies that are already committed to the principles does not alone accomplish that goal. That is why the Global Network Initiative includes not only an independent assessment process, but new commitments among companies, human rights groups, investors and academics to collaborate to promote the rule of law and freedom of expression and privacy.

We believe strongly that, in order to be truly effective against government censorship, a broad, diverse, and global group of companies, human rights groups, and other stakeholders must work collaboratively to advocate before governments and international bodies to ensure that the principles of freedom of expression and individual privacy are respected by governments around the world.

6. What policies or practices does Google have in place to protect user privacy and freedom of expression in foreign countries?

As part of our commitment to making the world's information universally accessible and useful,

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00070 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.031

Google takes seriously the protection of user privacy and freedom of expression in all the countries where we offer our products and services. Our general strategy includes three primary elements:

- **Political and legal environment.** In addition to business opportunities, we consider the political, legal, and human rights landscape of the countries where we offer our products and services. Among a number of factors, we consider whether a country's laws support free expression and individual privacy, whether the country operates under the rule of law, and whether individuals are empowered to protect their rights in the country's judicial system.

- **Technology and infrastructure.** As we design and localize our products, we strive to provide robust information and communication tools while offering technology features that protect user privacy and maintaining an infrastructure to keep user information secure. For example, in countries where we offer our Google Talk instant messaging service, we offer users the ability to go "off the record" so that their chats are not saved in Google's systems or their own computer. Likewise, we strive for transparency regarding our policies. In China, for example, we made the innovative decision to provide a notice to users of when we remove search results in compliance with Chinese laws, regulations, and policies.

- **Legal review.** Trained teams conduct careful review of all government requests to remove content or disclose personal information, as described in detail below.

With respect to our review of government requests for data, Google has dedicated teams within its legal department for receiving, evaluating, and responding to government requests to remove content from Google services or to provide information about Google users. These teams are global, multi-lingual, and cross-functional to ensure prompt and effective responses to such requests. The legal support teams are specifically trained by and under the supervision of senior Google attorneys. Government requests that appear to infringe upon individual freedom of expression or individual privacy are carefully reviewed and escalated to a supervising attorney and, in some cases, to Google executives.

In reviewing government requests for the removal of content from a Google product, our trained legal support team responds to all court orders or other government requests seeking removal of content. Each complaint is reviewed for procedural and substantive validity. In matters where the content violates a specific country's law, Google's policy is to narrowly remove content whenever possible. For example, a search result linking to Nazi material in violation of German law is removed from the German (or .de) domain, but not from all country domains. In circumstances where the content at issue is on a global .com domain (for example, on www.youtube.com), Google endeavors to narrowly block the display of content only in the jurisdiction where such content is illegal and to leave the content available for the rest of the world.

Google takes seriously all requests for the disclosure of information about its users. We design our products with user privacy in mind and only collect and maintain information as appropriate to provide the service. Many of our products do not require any personal information in order to use them. To the extent we have information about a user, Google's policy is to require valid legal process before providing any personal information to government authorities. In regard to non-U.S. requests for user information, in countries where Google has an office or other legal presence, local attorneys review the request to ensure that it complies with local law. Once valid legal process is confirmed, the request is passed to a trained team in Google's U.S. headquarters for further review

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00071 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.032

and, if appropriate, processing.

7. How will Google respond if during the Olympics the Chinese government asks you to identify a non-Chinese journalist who uses his Google.com Gmail account from an Internet cafe in Beijing to send what the Chinese government considers sensitive information to his editors in another country?

Google did not receive any such request. Had we received such a request from the Chinese government, we would have operated pursuant to the Mutual Legal Assistance Treaty or equivalent executive agreement between the U.S. and China. We made this commitment to Senators Durbin and Coburn by letter dated August 1, 2008, in which we stated that we would not provide to the Chinese government with any sensitive personal information about American athletes, journalists, or tourists during the Beijing Olympics unless required to do so by U.S. law pursuant to the MLAT or other equivalent executive agreement between the U.S. and China.

8. Google's witness at "The Internet in China: A Tool for Freedom or Suppression," the House International Relations Committee hearing on February 15, 2006 (2006 HIRC hearing) testified "As a practical matter, when we hear from government officials about how they define; the laws and what they define compliance to mean, we generally accept that." Is that still Google's practice or do you make an independent assessment of whether a request from a foreign government complies with the foreign government's law?

Google has a long-standing policy of ensuring that government requests are valid, legal, and binding. Furthermore, it is our policy and our practice to make case-by-case assessments, to the extent we are in a position to do so, of whether requests from a given government comply with that government's laws.

9. You testified that Google.cn does not offer Gmail or Blogger because Google might be required to provide personally identifiable user information to the Chinese government. However, Google.com offers Gmail and Blogger to users around the world, including in China. What process does Google follow when you receive a request from a foreign government for the personally identifiable information of a Gmail.com or Blogger.com user in that country?

Please see our answer to question 6 above. In the specific case of China, we do not store our users' Gmail and Blogger-related personal and confidential information in China, and we would refuse to provide such information to the Chinese government except pursuant to the Mutual Legal Assistance Treaty or equivalent executive agreement between the U.S. and China. Because we take the issue of user privacy and security very seriously and believe that offering more communication platforms in China and other countries promotes free expression, we continue to dedicate considerable effort into developing ways to expand the offering of such products while minimizing risks to users.

10.

a. Please provide a list of all the localized services that Google offers.

We offer several of our products in localized versions that are identified with a country's country

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.033

code top-level domain (*e.g.*, .ca for Canada and .mx for Mexico). In addition to Google Search, which we offer in 153 localized versions, we offer localized versions of products like YouTube, Chrome, orkut, Google News, Google Groups, Google Earth, and iGoogle.

b. Which of these localized services host Gmail, Blogger, and Orkut?

Though Google offers Gmail in over 50 languages and Blogger in over 40 languages, we do not offer localized versions of these products. We currently offer localized versions of orkut on country domains for Brazil and India only.

11.

a. What process does Google follow when you receive a request from a foreign government for the personally identifiable information of a user of the localized service' Gmail, Blogger, or Orkut?

Please see our answer to question 6 above.

b. In what circumstances would you decline or challenge in court such a request?

Each government request for personally identifiable information is reviewed by a trained member of Google's legal department for both procedural and substantive validity. If the requested data is not available in the country or if the request is not procedurally or substantively valid, Google may decline or challenge such a request.

c. Have you ever declined or challenged such a request? Please explain.

As described above, Google's policy is to require valid legal process before providing any personal information to government authorities. As a matter of practice, Google regularly engages law enforcement and other government authorities when they request user information and challenges or declines requests that are substantively or procedurally deficient.

For example, in June 2007, we received an informal request from the Royal Thai Police investigating several videos on YouTube that allegedly violated the Thai law prohibiting criticism of the Thai King, Bhumibol Adulyadej. In particular, the police sought the Internet Protocol (IP) addresses and other non-public information of the users who uploaded the videos. Google declined to provide such information and referred the police to the Mutual Legal Assistance Treaty or letter rogatory process – a process which works through the U.S. State Department – in order to obtain information.

d. Who at Google is ultimately responsible for authorizing the disclosure of personally identifiable user information?

Government requests that appear to infringe upon individual freedom of expression or individual privacy are carefully reviewed and, where appropriate, escalated to a supervising attorney and, in some cases, to Google executives.

12. According to media reports, Google recently helped authorities in India to identify

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.034

Rahul Krishnakumar Vaid, who allegedly posted vulgar comments about Indian official Sonia Gandhi on Orkut. Under Indian law, Mr. Vaid could face up to five years in prison.

a. Why did Google provide information about Mr. Vaid to the Indian authorities?

As a threshold matter, there is a significant difference between the situation of Mr. Vaid and cases of the investigation and prosecution of cyberdissidents in other countries. India is a representative democracy with an independent judiciary and due process of law. By contrast, certain regimes that censor political and religious expression – on the Internet and through other media – are often not democratic or bound by the rule of law.

We believe that it is important to acknowledge that democracies can pass laws regarding pornography and obscenity laws and other laws that limit freedom of expression – and, indeed, Mr. Vaid's case involved Indian obscenity laws. However, we believe that it is incorrect to suggest equivalence between democracies bound by the rule of law and undemocratic regimes. We also believe that it is important to underscore that U.S. companies cannot necessarily impose American legal standards on communications platforms operating in other countries, any more than foreign companies can impose their legal standards in the U.S.

Freedom of expression can best be promoted if significant groups of companies and other stakeholders work together to establish best practices with the hopes that they will be broadly adopted, and – maybe more importantly – if countries that respect and uphold principles of free expression work within the international community to ensure that these principles are respected and upheld globally.

In Mr. Vaid's case, Google provided only limited subscriber and IP address information about his orkut account to police investigators in Pune, India, where prosecutors charged Mr. Vaid under Section 292 of the Indian Penal Code and Section 67 of the Information Technology Act, 2000. The laws criminalize the publication of obscene materials on the Internet and through other media. Google provided information relating to Mr. Vaid's account to the investigating Indian authorities because the request for information in our assessment constituted valid legal process under Indian law.

b. Please explain the process Google used to handle this request.

We followed the process described in our answer to question 6 above.

c. Did Google make an independent assessment of whether the request complied with Indian law?

Yes, Google made an independent assessment informed by our outside legal counsel in India that the request from the Pune police for information about Mr. Vaid was valid legal process under Indian law.

d. Did Google evaluate whether complying with the request would lead to Mr. Vaid being prosecuted for exercising his right to free expression?

Yes, Google did conduct an evaluation of whether complying with the request could lead to his

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.035

prosecution under Indian law.

e. Did Google consider challenging the request in Indian courts?

Yes, and we concluded that the request in question was valid under Indian law, not likely to be overturned on appeal, and that an appeal on the facts might be counterproductive to the larger cause of free expression because it could result in harmful legal precedent.

f. If you determined that a request from Indian authorities violated Indian law, would you challenge the request in court?

It would depend upon a number of factors including but not limited to the facts of the specific case, the advice of counsel qualified to practice Indian law, and the likelihood of success versus the possibility of establishing a counter-productive precedent in the emerging area of online legal speech.

g. Where was the information about Mr. Vaid physically stored?

The orkut service is owned and operated by Google Inc. and the data regarding Mr. Vaid was located on servers in the U.S. As such, the governing U.S. law for user information stored in connection with orkut – as with other electronic communications services – is the Electronic Communications Privacy Act. Under ECPA, service providers may disclose a limited subset of user information to third parties, including foreign governments. When Google receives valid legal process from a government in a country where we do business and which operates under the rule of law, we may provide such limited information to local authorities.

13.

a. In addition to Google.cn, for which other localized services do you censor political or religious content?

As stated in Nicole Wong's testimony before your Subcommittee, German law makes Nazi content illegal, so we remove such content from our products hosted on our German domain, Google.de, when we become aware of such material. However, we do not remove Nazi content because of German law from our global products hosted on Google.com. Likewise, we have removed content from localized services for Austria, Belgium, Brazil, Canada, Czech Republic, France, Germany, Israel, Poland, Switzerland, and the United Kingdom in accordance with the hate speech laws in those countries. In addition, we have terms of use and guidelines for user-generated content that is hosted by Google. For example, YouTube's community guidelines encourage free speech, including unpopular points of view. However, hate speech (speech which attacks or demeans a group based on race or ethnic origin, religion, disability, gender, age, veteran status, and sexual orientation or gender identity), and speech that is likely to lead to violence is not permitted on YouTube.

b. For each of these localized services, how do you determine what to censor?

In each of the above cases, Google conducted an independent legal analysis of relevant laws and our obligations under those laws. We then proceeded to remove content that we believed violates relevant national laws. In addition, we regularly receive reports from third parties of content on

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.036

local domains that allegedly violate national laws. In each of these cases, Google conducts an independent analysis of the report, determines whether the content reported violates the law, and acts accordingly.

c. What process does Google follow when you receive a request from a foreign government to censor political or religious content?

In general, for localized services Google conducts an independent legal analysis of relevant laws and our obligations under those laws. If appropriate, we then proceed to remove content that we believe violates relevant national laws. For example, in 2007, we received demands from authorities in Mumbai, India, to remove an orkut community that criticized a popular but violent religious sect known as Shiv Sena and its leader. In addition, the Mumbai police threatened to arrest local Google employees, supporters of Shiv Sena rioted outside of the Google office in Mumbai, and police detained Google's counsel for more than a day. We consulted with local counsel to confirm the validity of the police request and its authority under Indian law. After further evaluation by our U.S. legal team, we removed the communities that were confirmed as illegal. Our analysis may differ when the demand comes from a government where we do not have localized services or a business presence. Please see our response to question 13(e) below.

d. In what circumstances would you decline or challenge in court such a request?

In general, we would decline or challenge in court such a request when it appears that removing the content in question does not violate relevant national laws. For example, in Turkey, prosecutors and the Turkish Telecommunications Authority have repeatedly demanded the removal of videos on YouTube that allegedly criticize Mustafa Kemal Ataturk, the founder of the Turkish republic, or "Turkishness" which is prohibited by law. Under court order, the Turkish Internet Service Providers have blocked the entire YouTube site multiple times over the last year. Indeed, YouTube has been blocked in Turkey for the last four months. Although we have offered to block videos for IP addresses in Turkey when those videos violate Turkish law, the prosecutors have stated they are not satisfied with such measures and insist upon the global removal of these videos. To date, we have declined to make those removals and we remain blocked in Turkey, and we continue to engage with the Turkish government on this matter.

As another example, earlier this year, the government of Tunisia requested that Google remove from its Google Earth product the satellite image of the Presidential Palace and accompanying user comments that are critical of the Tunisian President. We explained to the Tunisian officials that Google is not operating in Tunisia and not subject to Tunisian law and, thus, we would not be removing the content.

e. Have you ever declined or challenged such a request? Please explain.

In 2007, YouTube users outside Thailand uploaded several videos to the site containing political commentary on Thailand's military regime and royal family, including the country's revered king. In one video, for example, the Thai king's face was altered to resemble a monkey and feet were displayed next to his face, a severe insult in Thai culture.

Thailand is one of the few remaining countries to enforce actively a law of *lese majeste*, prohibiting insults to the king. As a result, the Thai minister of communications ordered Thai ISPs to block

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.037

access to the entire YouTube site, which became inaccessible to users within the country. This censorship had the unintended effect of blocking videos Thai users had posted in response expressing outrage and defending their king.

We opened a dialogue with the Thai ministry and requested a list of the allegedly illegal videos. With the benefit of video-by-video analysis from local counsel, we ultimately agreed to block from Thai IP addresses the videos that plainly violate the law of *lese majeste*, but declined to block videos critical of the military regime but not the king. While the government asked for the complete removal of this content, it is our policy, when we agree to limited blocking, to only narrowly block videos within the country where such material is illegal. We believe strongly that a given country's limitations on free expression should not affect users in other, less restrictive countries.

f. Who at Google is ultimately responsible for authorizing the censorship of political or religious content?

Government requests that appear to infringe upon individual freedom of expression or individual privacy are carefully reviewed and, where appropriate, to a supervising attorney and, in some cases, to Google executives.

14. At the hearing, I asked about the Chinese government's attempts to suppress information about the SARS epidemic. In the event of another public health emergency in a country that suppresses such information, how would Google respond to a censorship or takedown request regarding information about that health threat?

If it were clear from the face of a given filtering request that an attempt was being made to suppress information relevant to a public health emergency of SARS-like proportions, Google employees would escalate the issue to senior legal personnel in Google's U.S. headquarters. Google's senior legal personnel would, in turn, evaluate the request, taking into the legality and validity of the request, the need to communicate information about the situation, and any legitimate government purposes such as wanting to avoid panic or incorrect rumors that could harm public health efforts.

15. How do you determine what content should be censored on Google.cn?

As has been described in various reports and news articles, commercial web services operating in China – and, in particular, search engines – are held responsible for monitoring their own services. This monitoring and filtering is performed primarily in response to and pursuant to government requests. These requests typically are for the removal of certain content or for the restriction of access to certain content.

In Google's case, we have two search services that are available in China. The first is our global search service, Google.com, which is available in Chinese. The second is our localized search service, Google.cn. Google.com is available in China, except when it is blocked. Google.cn has faster performance, but it also has certain results censored in accordance with Chinese laws, regulations, and policies.

The goal of offering the Google.cn service is to provide more information and transparency to Chinese users than they otherwise would receive. However, a small percentage of search results are

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.038

filtered. These typically relate to topics deemed sensitive in China, such as Tiananmen Square, Tibet, and Falun Gong. We endeavor to filter results in a way that minimizes censorship, and we believe that we filter less than our competitors in China. We also believe that we provide significant transparency to our users in China, and we are working hard to improve transparency to our Chinese users.

Government requests to filter content may refer to specific keywords, combinations of keywords, uniform resource locators (URLs), and topics. Requests relating to content appearing on google.cn are processed by Google's China joint venture, which may contact the requesting authority to discuss whether a filtering request can be implemented in a less restrictive manner. Joint venture employees try to minimize filtering by limiting responses to a restricted set of websites in the overwhelming majority of cases, rather than blocking all responses, and by narrowly interpreting requests to filter results on certain topics. The employees also regularly review what is being filtered to determine whether keywords and URLs can be removed, generally based on whether relevant information is otherwise available on the Internet.

A Google employee receives reports of filtering activity. The Google employee reviews these reports to see whether filtering is being done in a manner that is inconsistent with Google's core values.

According to the most recent internal testing comparing google.cn search results with those of other major search engines in China, google.cn's results are the least restrictive. In addition, less than 0.3% of queries are filtered, and the overwhelming majority of filtered keywords relate to pornography and other non-political content. A 2006 Reporters Without Frontiers report indicates that google.cn censors less than search competitors in China. (Report located at http://www.rsf.org/article.php3?id_article=18015.) A more recent report published last month by Nart Villeneuve, a University of Toronto internet researcher, substantiates the 2006 Reporters Without Frontiers. (Report located at http://www.citizenlab.org/papers/searchmonitor.pdf.) That report states:

> Internet users in China are able to retrieve a slightly wider array of content (20% more, on average) due to the presence of foreign search engines. . . When the results from Google, Microsoft and Yahoo are combined, 20% of the sites censored by Baidu are available. However, individually they provide more information, especially Google and Microsoft . . . Google maintained the lowest average number of censored sites at a rate of 15.2% and was closely followed by Microsoft 15.7%. Baidu ranked the highest at 26.4% and Yahoo! averaged 20.8%.
>
> Users are provided with clear notice when google.cn filters search results. The full, unfiltered results are still available on google.com. The google.cn homepage links to google.com, which is offered in Chinese and provides unfiltered information when it is available to users in China.

a. During the 2006 HIRC hearing, Google's witness said that Google initially determined what to censor on Google.cn "by looking at the performance of the filtering of government authorities." Is that still how Google determines what to censor on Google.cn?

Please see our answer to question 15 above.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.039

b. Has the Chinese government ever given Google any direction or guidance regarding what to censor?

Please see our answer to question 15 above.

16. You testified, "in China, we believe we are the least filtered, most transparent search engine available," Google co-founder Sergei Brin recently defended Google's activities in China by saying, "Google has a far superior track record than other search companies with respect to making information freely available." What is the basis for your and Mr. Brin's claim that: Google.cn filters less and makes more information available than other search engines in China?

Please see our answer to question 15 above.

17. You testified that "whenever we offer censored results on our Google.cn search engine, we present clear notification on the results page to users." You also noted that, "After we did it, the other major search engines in China are now having a similar type of notice." Since other search engines in China now provide a notice of censored results, what is the basis for your claim that Google.cn is the most-transparent search engine in China?

As a threshold matter, the fact that our presence in China has led to greater transparency even from our local competitors is a very positive development. Our engagement in China through Google.cn has driven industry advances in transparency to users. Today, leading search engines in China, including the market leader Baidu, have followed our lead and now provide disclosures when they remove results.

This was not the case before Google.cn established this practice with its launch in 2006. This fact is noted by the Villeneuve report, which states, "Since this report was finalized, the domestic Chinese search engine Baidu, following the foreign search engines, introduced a censorship notification [located at http://blockpage.com/main.php?g2_itemId=135] indicating that it is possible to make progress through engagement." To build on these accomplishments, Google continues to focus on increasing transparency in Google.cn, for example by stating more clearly that at times we do not provide results because we are unable to do so, rather than merely saying that we are not providing results.

18. Human Rights Watch's Arvind Ganesan testified, "disclosing censorship is not enough, but actually actively trying to reduce it to where your minimum level is whatever the government says it is." Please describe what Google has done to reduce censorship to the minimum level.

Google's mission is to make the world's information universally accessible and useful. As such, we view our products as powerful vehicles for reducing censorship around the world because they enable access to and communication of information for anyone in the world with an internet connection. We have seen – in Myanmar, Venezuela, Egypt, and many other countries – the power of the Internet to elude government censorship. Furthermore, as described in our responses above, we approach specific government demands to censor seriously and we make any removals required narrowly by localizing it to a specified country domain or country IP addresses. Also, please see our

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.040

answer to question 15 above.

19. Global Internet Freedom Consortium's Shiyu Zhou testified, "for companies like Google and Yahoo!, there is self-censorship in China I would say is more damaging than other kinds of censorship, because for Chinese people in such a closed society, they take Google and Yahoo! as role models of freedom of information. When they look on the websites and they find the information, they believe it is factual and it is true." Do you agree?

We agree that there are cases where American internet companies should operate in countries that censor, in large part because companies like Google represent a culture of more access to information, more debate, and more free expression. In addition, companies like Google can serve as a check on the practices of local competitors. And if American companies do not provide search services, video sharing services, blogs, and other internet products and services, local competitors will do so. We know that this is true in countries like China, where Google and other American companies face strong competition from local companies that sometimes benefit from strong relationships with and the patronage of the government.

We also agree with Mr. Shiyu's suggestion that censorship runs contrary to our mission statement, which is to organize the world's information and make it universally accessible and useful. In China, we have chosen the imperfect solution of offering a filtered search service through Google.cn because we believe that, on balance, it is better for Google to offer all but a handful of information to users in China than to not provide our search at all. To this day, our Google.com search service is regularly blocked or degraded in China, and without Google.cn Chinese users would not have regular access to our search engine.

It is important to emphasize that our search service is focused on providing access to information, not on passing judgment on the information. This is important because for Google's search service to be useful, it must provide results that our users are looking for.

If legal restrictions in a particular country stop us from providing certain results, then the most important action that we can take on behalf of our users is provide them with transparency – a statement that we have not provided complete results and that certain results have been omitted. This is what we do in China when we filter results on Google.cn, and as a result users of Google.cn know that there is additional information that exists and can be accessed – for example through Google.com, which is offered in Chinese and to which we provide a link on the Google.cn homepage.

20. Please provide a copy of any human rights guidelines, policies, and training that Google has in place.

Though our current materials are internal and confidential, the GNI documents that we recently signed onto are public and available at www.globalnetworkinitiative.org. The GNI documents, which consist of Principles, Implementation Guidelines, and a Governance, Accountability & Learning Framework, will serve as the framework for our internal documents as we implement GNI. We would be happy to discuss specific questions that your staff may have about our internal documentation at their convenience, and we will make sure to share with you our progress as we implement GNI.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00080 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.041

21. You testified about Google's "current practice of conducting risk assessments that consider the impact on free expression and other human rights of entering new markets or introducing new products into existing markets." Please provide more information about these risk assessments, including for what new markets or new products you have conducted such assessments, how you conduct such assessments, and how the results of such assessments have affected whether to enter a new market or introduce new products into existing markets.

When we consider entering new markets, we conduct risk assessments that touch on a wide range of factors, including business environment, internet access, and internet use statistics. In addition, we evaluate the legal environment, rule of law, and substantive laws and regulations relating to data protection and privacy, freedom of expression, and human rights more broadly.

Our primary assessments are drawn from two sets of sources: (a) third-party evaluations such as the categorical ratings produced by the World Bank, Freedom House, Transparency International, the OpenNet Initiative, and Reporters Without Borders, as well as the annual country reports of Human Rights Watch, Amnesty International, and the U.S. Department of State, and (b) input from both in- and out-of-country experts in academia, business, trade associations, NGOs, and advisory and law firms.

For new product issues, these assessments are typically tailored to the specific product proposals or ideas. For larger decisions about new markets, the assessments take the form of intensive country reviews. In one form or another, we have assessed conditions in nearly every country on the planet. Our risk assessments have informed and shaped our decisions across many markets and product issues.

22. You testified, "We do not have an investment in Baidu. .. I believe we did previously and sold off the investment a few years ago. I can check that out for you." Please explain.

Shortly prior to Google's initial public offering in 2004, the company purchased a small equity stake in Baidu. We divested our 2.6 percent interest in Baidu in June 2006.

23. At the 2006 HIRC hearing, Google's witness testified that Google decided to start a censored China service due to "our steadily declining market share" in China. He explained that Baidu, your largest Chinese competitor, had risen to 46% of the market share in 2005, while Google had dropped 'to below 30%. Has your decision to launch Google.cn helped Google to regain market share? What are the market shares of Baidu and Google.cn today?

Our share of internet searches in China has decreased steadily from early 2005, when we reportedly had a 33 percent share. This share dropped to a low of 12 percent in 2006 when Google's website was blocked by the Great Firewall. With the development of the Google.cn website, our search share has stabilized at approximately 21 percent. In the meantime, Baidu has launched many community and messaging products, and these additional product offerings have propelled Baidu's share to over 73 percent.

We believe that our commitment not to store personally identifiable information unless it can be appropriately handled has harmed our business in China, reducing the range and value of services we can offer users. This harms not only our search business, but our ability to compete with local

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.042

competitors in other online services, such as webmail, bulletin boards, etc. For example, Baidu has more flexibility to launch localized services because it does not impose on itself the same restrictions that we impose on ourselves with respect to storing personally identifiable information in China.

However, as noted in previous answers, we believe that our localized presence in China has led to more transparency and less censorship for Chinese internet users. Though we would like to be more competitive in the Chinese market, we believe that these positive developments are, in and of themselves, significant accomplishments.

Question from Senator Sam Brownback

You indicate in your testimony that Google's goal is to "mak[e] sure that the Internet is a global platform for free expression." You assert that "our products are above all else platforms for free expression and access to information." Does that include free expression by terrorists and access to how-to guides for terrorists?

YouTube's policies prohibit users from uploading videos that contain hate speech and threats of violence against specific individuals or groups. Our policies also prohibit videos that promote dangerous or illegal activities (including bomb making, sniper attacks, or other terrorist acts), and videos that are posted with the purpose of inciting others to commit specific, serious acts of violence.

I understand that Google's YouTube makes Al-Qaeda training and propaganda videos available to users. These videos incite violence against the United States and other democracies throughout the world. What is Google's policy regarding accessibility to these videos?

YouTube's Terms of Use require all users to abide by our Community Guidelines before uploading videos. The Community Guidelines prohibit hate speech, threats of violence against specific individuals or groups, the promotion of dangerous or illegal activities (including bomb making, sniper attacks, and other terrorist acts), and content posted with the purpose of inciting others to commit specific, serious violent acts.

YouTube staff review videos flagged for violating our guidelines 24 hours a day, seven days a week. When we determine that content violates our guidelines, we act quickly to remove it. We also disable the accounts of repeat offenders.

What, if any, steps has Google taken to remove these videos? Please explain the rationale behind the steps Google has taken to remove these videos.

Every minute, 13 hours of video are uploaded to YouTube, totaling hundreds of thousands of videos every day. We cannot and do not review content before it goes live, anymore than a telephone company screens the content of calls before they are made, or an ISP edits emails before they are sent.

Practically speaking, the only way we can offer YouTube at the scale we do is to rely on our user community to effectively police the site for inappropriate content. We have developed an innovative and reliable community policing system that involves our users in helping us enforce our content policies. Because our global community never sleeps, there is no bigger or more

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00082 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.043

comprehensive group in the world to identify inappropriate content on our site. Millions of users report potential policy violations by selecting the "Flag" link while watching videos.

All videos, including terrorist videos, brought to our attention through community flagging are reviewed against our content policies 24 hours a day, seven days a week, and typically in under an hour on average. We regularly remove videos that contain hate speech or threats of violence against specific individuals or groups, videos that promote dangerous or illegal activities (including bomb making, sniper attacks, and other terrorist attacks), and videos that are posted with the purpose of inciting others to commit specific, serious violent acts.

Specifically, we have removed several hundred videos that depict, among other things, attacks on U.S. military vehicles, hostages held in captivity, sniper attacks, and beheadings.

If Google is allowing any terrorist videos to remain on YouTube, please explain in detail the rationale behind this decision.

YouTube's content policies include prohibitions on hate speech, graphic or gratuitous violence, threats of violence against specific individuals or groups, as well as videos that promote dangerous or illegal activities (including bomb making, sniper attacks, and other terrorist attacks), and videos that are posted with the purpose of inciting others to commit specific, serious violent acts. When flagged, videos that contain such content are promptly removed.

Additionally, it is YouTube's policy to remove all videos and terminate any account known to be registered by a member of a designated Foreign Terrorist Organization (FTO) and used in an official capacity to further the interests of the FTO.

Questions of Senator Tom Coburn

In testimony before the House panel in February 2006, Google testified about its approach to China, describing the situation as presenting "only imperfect options." At the time Google, felt that its decision to do business in that country was reasonable, but stated that, "If we determine that we are unable to achieve the objectives [we've outlined], we will not hesitate to reconsider our approach to China." Now, more than two years later, how does Google feel about its approach to doing business in China?

In our February 2006 testimony before the House Committee of Foreign Affairs we stated that our approach is not the "single 'right' answer to the dilemma faced by information companies in China, but rather a reasonable approach that seems likely to bring our users greater access to more information than any other search engine in China."

We believe that our decision to operate the Google.cn search service has been, on balance, the right one because our presence in China has led to improvements in freedom of expression. For example, we believe that more internet users in China can access more information outside of China through Google.cn than through other offerings.

And we work very hard to make sure we censor less in China than our competitors. According to the most recent internal testing comparing google.cn search results with those of other major search engines in China, google.cn's results are the least restrictive. In addition, less than 0.3% of queries

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00083 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.044

are filtered, and the overwhelming majority of filtered keywords relate to pornography and other non-political content. A 2006 Reporters Without Frontiers report indicates that google.cn censors less than search competitors in China. (Report located at http://www.rsf.org/article.php3?id_article=18015.) A more recent report published last month by Nart Villeneuve, a University of Toronto internet researcher, substantiates the 2006 Reporters Without Frontiers. (Report located at http://www.citizenlab.org/papers/searchmonitor.pdf.)

That report states:

> Internet users in China are able to retrieve a slightly wider array of content (20% more, on average) due to the presence of foreign search engines. . . When the results from Google, Microsoft and Yahoo are combined, 20% of the sites censored by Baidu are available. However, individually they provide more information, especially Google and Microsoft . . . Google maintained the lowest average number of censored sites at a rate of 15.2% and was closely followed by Microsoft 15.7%. Baidu ranked the highest at 26.4% and Yahoo! averaged 20.8%.
>
> Users are provided with clear notice when google.cn filters search results. The full, unfiltered results are still available on google.com. The google.cn homepage links to google.com, which is offered in Chinese and provides unfiltered information when it is available to users in China.

In addition, our engagement in China through Google.cn has driven industry advances in transparency to users. Today, leading search engines in China, including the market leader Baidu, have followed our lead and now provide disclosures when they remove results. This was not the case before Google.cn established this practice with its launch in 2006. This fact is noted by the Villeneuve report, which states, "Since this report was finalized, the domestic Chinese search engine Baidu, following the foreign search engines, introduced a censorship notification [located at http://blockpage.com/main.php?g2_itemId=135] indicating that it is possible to make progress through engagement."

Does Google collect or store personally identifiable information on users in China or elsewhere who simply search the web? In other words, if I live in China and frequently search the terms "Falun Gong" or "Tibet freedom," should I worry that the Government could discover my identity? If they did, would it be a crime?

We do not offer search services – or email or blogging services – that store our users' personal information in China. For example, a user in Beijing could open a Gmail account, but the emails that the user composed, sent, and received using that service would not be stored in China. Because of this policy, we do not believe that we can be compelled to turn our users' search-related information over to Chinese authorities and we would not do so except pursuant to the Mutual Legal Assistance Treaty or equivalent executive agreement between the U.S. and China. In order to provide more products in China, which we believe is important to enhancing free expression in that country, we continue to look for alternative ways to let users provide information with full notice and transparency as to the risk that it could be subject to disclosure to the government.

* * * * *

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00084 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.045

Senate Judiciary Committee
Subcommittee on Human Rights and the Law
"Global Internet Freedom: Corporate Responsibility and the Rule of Law"
May 20, 2008

Questions for the Record – Shiyu Zhou, Global Internet Freedom Consortium

Questions from Senator Tom Coburn:

1. In your opinion, can communication services like email or blogging sites ever be used safely — in other words, without the risk of identifying cyber dissidents — in countries like China?

Answer: Yes, they can be used safely even in China, if users effectively take advantage of end-to-end anti-censorship tools like the Global Internet Freedom Consortium (GIF) provides. Starting from account registration, to downloading emails or posting blogs, to visiting other sites, users have to use secure anti-censorship tools to hide their identity.

Of course, it would be even safer if users can use the email services and blogging sites GIF has been providing, which resides in the United States but with their native language interface, and is a full end-to-end solution when users use our anti-censorship tools to access these services.

2. Google rightfully prides itself on transparency — that even though it must sometimes censor in compliance with local laws, it provides a notice to let its customers know what has been done. Would a similar disclosure be effective for users of communication services like email or blogging? Perhaps a notice disclosing the fact that the Internet service provider must operate in compliance with local law and that information exchanged may be subject to government review?

Answer: It is not transparency, it is censorship. In fact, Chinese Internet police have been doing it by forcing ISPs to place images of big-eyed net police cartoons on their websites. Chinese Internet users have already lost their trust in the domestic ISPs. Even for foreign ISPs, since the Shi Tao-Yahoo incident, Chinese users no long trust them. But that does not mean they do not need safe, secure email and blogging services, and that is why GIF has been providing such services to censored users.

3. Would you please submit to the subcommittee all evidence you have showing Cisco's alleged cooperation with the Chinese Government?

Answer: Yes. We have submitted some materials already. Attached is some additional info:

(1) psindustryknowledge_Eng.pdf gives an overview of the Public Security

45688.046

Industry of China, and lays out the marketing strategy for Cisco-China to sell products and solutions to the Chinese police.

On page 57, it reveals that one of the major objectives of the GSP is to "combat 'Falun Gong' evil cult." On page 58, it shows that Cisco offers much more than just routers; it offers planning, construction, technical training, and operations maintenance for GSP.

(2) GSP-background-English.pdf gives an overview of the needs of GSP and Cisco's high-level solutions meeting the needs.

(3) The Cisco_Chronical (translated from the Chinese version on Cisco's website) shows that Cisco not only helped the Chinese authorities construct the level-2 and level-3 of GSP, but also did level-1, which is the backbone of GSP.

(4) Cisco-and-1st-Level-GSP.rtf (translated from the Chinese version on Cisco's website) explains more details on how Cisco helped the Chinese authorities construct level-1 backbone of GSP.

(5) The translation of the two paragraphs in the Chinese version of Wikipedia on GSP (which are missing in the English counterpart of Wikipedia) explains that China's Great Firewall is part of the GSP.

45688.047

SUBMISSIONS FOR THE RECORD

Written Testimony of Amnesty International USA
Before the Senate Committee on the Judiciary Subcommittee on Human Rights and the Law
on "Global Internet Freedom: Corporate Responsibility and the Rule of Law"
May 20, 2008

Amnesty International is a Nobel prize-winning human rights organization with over 2.2 million members worldwide and over 300,000 in the United States. For over 40 years, Amnesty has worked to promote and defend internationally recognized rights encompassed in the Universal Declaration of Human Rights (UDHR), including freedom of expression and privacy.

Under the UDHR, all companies, as organs of society, have a direct responsibility to respect human rights in their own operations. Amnesty International believes that the business community also has a wider responsibility -- moral and legal -- to use its influence to promote respect for human rights.

It is with these understandings that Amnesty International began to monitor and report on the role of U.S. companies in repression of freedom of expression and privacy on the Internet. In February 2006, Amnesty testified before Human Rights Caucus of the United States Congress on the subject of human rights and the Internet in China. At that time, Amnesty discussed the role of U.S. companies in repression of freedom of expression abroad, including Cisco Systems and Sun Microsystems, which have helped to build the infrastructure that makes Internet censorship possible, and Yahoo!, Microsoft, and Google, which comply with government requests to censor information and hand over users' personally identifying information.

In July, Amnesty issued a report entitled *Undermining Freedom of Expression in China: The role of Yahoo!, Microsoft and Google*. The report concluded that all three of the named companies failed to live up to two fundamental human rights principles embodied in the UN Global Compact: First, that businesses should support and respect the protection of internationally proclaimed human rights within their sphere of influence, and second, that businesses should ensure that their own operations are not complicit in human rights abuses.

Since the issuance of the report, U.S. companies have continued to aid repression of the Internet, resulting not only in untold violations of people's rights to seek, impart and receive information, but also in continued protests from the public at large. Amnesty presented the signatures of 50,000 people to the 2006 United Nations Internet Governance Forum calling on governments to stop the unwarranted restriction of freedom of expression on the Internet – and on companies to stop helping them do it. Additionally, before and after the Forum, tens of thousands of Amnesty members have written to the companies named in the July report, pleading with them to stand up against repressive governments

45688.048

and to abstain from helping them violate freedom of expression and privacy rights of people around the world.

To help companies realize the goals of protecting, promoting and respecting freedom of expression and privacy in their own operations and within their sphere of influence, in January 2007, Amnesty joined a multi-stakeholder initiative with Internet and telecommunications companies, other human rights groups and non-governmental organizations, socially responsible investment firms and academic institutions to help develop a set of principles on freedom of expression and privacy for the industry. From the beginning of Amnesty's participation in the initiative, it has continuously called on companies to implement the recommendations of its July 2006 report, which, in addition to participating in a multi-stakeholder initiative, include:

- publicly committing to honoring freedom of expression and lobbying for the release of cyber-dissidents and journalists imprisoned solely for peaceful exercise of their rights to freedom of expression and privacy;
- exhausting all possible remedies and appeals before complying with state directives that would violate the rights to freedom of expression, access to information, and privacy;
- allowing for independent monitors to assess the companies' fulfillment of principles on freedom of expression and privacy;
- being transparent about filtering processes used to limit or restrict search results, including informing users and disclosing which terms are being censored;
- documenting and publicly disclosing cases where legally-binding censorship requests have been complied with; and
- developing human rights impact assessments, integrating them into business operations and disclosing their conclusions publicly

Some companies have painted our calls to action as unreasonable, and have misled their shareholders and the public to believe that Amnesty is asking them to stop operating in certain countries like China. This could not be further from the truth. Amnesty has called on companies to stand up to repressive regimes and to push back when those states push on them to abuse human rights. But rather than stand up to support human rights, internet companies have largely continued to choose to be a partner of repression.

Amnesty's work on business and human rights spans industries. Across a wide-range of firms, producing varying goods and services, it has become clear that when a company is committed to doing something, either because US law and regulation requires it or because it is important to the company, the company will find a way to produce results. It will make the commitment of resources. It will restructure itself internally. It will lobby governments.

It is not unreasonable for Amnesty International, other human rights groups, the US Congress, and the public at large to ask US Internet companies to do these things to protect the rights to freedom of expression and privacy.

Yet, nearly a year-and-a-half after officially joining the multi-stakeholder initiative with companies, Amnesty has seen internet censorship worsen in China. Internet access remains highly restricted, and websites are being shut down in the run-up to the Olympic Games. In this environment, Amnesty

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00088 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.049

questions how internet companies have made concrete changes in their operations that would prevent past abuses from reoccurring.

The multi-stakeholder initiative must not be used as an excuse for inaction. There is nothing in its mandate that precludes companies from taking proactive steps that might ameliorate Internet repression while conversations about standardized principles go on. Especially as the Games approach, it is more important than ever that US companies demonstrate leadership to ensure they are not a party to repressive tactics.

Further, the multi-stakeholder initiative should not be viewed as a replacement for much needed regulation. Many companies with operations that have significant impact on human rights are not members of the initiative, and even within the initiative, companies have demonstrated varying degrees of commitment to the exact accountability mechanisms that would make the principles credible.

Freedom of expression is not an abstraction. We should not allow companies or governments to desensitize its real significance for journalists and human rights defenders around the world whose courageous efforts to inform the public about government abuses provides everyday people with information necessary to make informed decisions about their lives, their government and their role within it.

Amnesty International welcomes the inquiry of the Subcommittee, and asks that it thoroughly probe into the level of commitment of the company witnesses to the recommendations for action outlined in this statement. Additionally, Amnesty International actively supports legislative efforts that would accomplish the same.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00089 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.050

Mark Chandler
Senior Vice President Legal Services, General Counsel and Secretary
Cisco Systems, Inc.
May 20, 2008
U.S. Senate, Committee on Judiciary
Subcommittee on Human Rights and the Law

Mr. Chairman, Members of the Subcommittee:

My name is Mark Chandler, Senior Vice President and General Counsel of Cisco. Thank you for the opportunity to address some very important and difficult issues that speak directly to the future of the Internet.

First, I'd like to share with you some background about the products our company is best known for. Networking equipment - routers and switches - forms the core of the global Internet and most corporate and government networks. Cisco has often been described as the "plumbers" of the Internet, as our technology constitutes the "pipes" that connect one location to another. Originally our products were designed for communications within private or corporate networks. When the public Internet emerged in the mid '90s, our products found immediate application for worldwide use. We now have many competitors around the world who build products that perform similar functions. When you send an email in your office to your children or grandchildren, the digital language that makes up that email is routed through equipment made by Cisco or our competitors

Over the last year, we have seen remarkable growth and transformation related to the Internet. The Internet continues to expand around the world and new applications such as collaboration tools and the use of video are transforming how we work, live, play and learn. More than 1.4 billion people now use the Internet, an increase of 300 million people in just one year. And new mobile devices such as the Apple iPhone have enabled millions of people to do what they want, when they want, with whom they want.

But at the same time, we have observed some troubling events and challenges related to the manipulation of Internet technology. Later this month will be the first anniversary of an unprecedented cyber attack that crippled the Estonian government and commercial networks. The attacks were labeled "cyber terrorism" and prompted NATO to create a new multi-national initiative to prevent such incidents. And in February, an ISP in Pakistan caused an international incident when it rerouted its computers to block YouTube from being watched in the country. The act had much broader implications by effectively hijacking the site for several hours worldwide. These incidents demonstrated that despite the Internet's redundant nature, it can still be disrupted by unilateral actions

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00090 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.051

and by cyberattacks. Every major corporate and service provider network is subject to nearly constant attack.

Attacks can take many forms, some of which are referred to as worms, viruses, denial of service attacks, and more. Network management and security capabilities are essential to mitigate attacks and thus enable information flow. No network can be administered by our customers without the ability to manage and protect the information that flows through it. Without this capability, it would not be possible to operate the Internet and the Internet would likely not exist as it does today. For example, without these tools, the Government of Estonia would have been powerless against the attacks it faced last year.

These tools are essential for many reasons. But the technology that is used to manage and protect against hackers or viruses is the same generic technology that filter or control Internet access by children, or the illegal downloading of copyrighted material. If, for example, a network administrator knows that a certain website is dangerous to her network because a virus or spyware has been downloaded from that site, or because the site is pornographic, she can use IP address blocking (each website and user on the Internet has an IP – Internet Protocol – address - the equivalent of a phone number) to protect her network from that site. This technology is a customary part of network management software of all major suppliers of Internet equipment -- Cisco's and our competitors' -- and is basic to network functionality. Whether for security or the management of information, the technology is one and the same. The filtering that occurs is implemented by the owner or administrator of the network using technology that is available regardless of the manufacturer.

In no country has the issue of the Internet and how it should be managed been more prominent than in China. China now has the largest Internet population in the world with 220 million users. There is no question that the Internet has been good for China and its people. It has provided unprecedented access to information. It's transforming China and its economy and it's helping the Chinese people engage more with the world.

Perhaps the most vivid example of the dramatic changes the Internet has brought to China is the response to last week's earthquake in the southwest region of the country. With mobile communications systems down or damaged, the Internet became a critical source of information for family and loved ones, as well as the rest of the world. Within minutes, pictures and videos from the region were online. That stands in stark contrast to the events in Tangshan 32 years ago, when the world received no official confirmation for months that a 7.8 magnitude earthquake had even happened, despite the deaths of an estimated 240,000 people and the destruction of much of that region.

As a company that supports free expression and open communication on the Internet, and believes that its products inexorably drive the world toward more open communication, Cisco respects the strength of conviction of those who bring concerns forward about efforts of various governments to censor freedom of expression on the Internet and persecute those who attempt to use the Internet for purposes of political speech. But we also must respond when Cisco is erroneously linked with these efforts.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00091 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.052

To set the record straight, it is important that the Committee understand that Cisco does not customize, or develop specialized or unique filtering capabilities, in order to enable different regimes to block access to information. Furthermore, Cisco sells the same equipment worldwide. Finally, Cisco is not a service or content provider, nor are we a network manager. Allegations that Cisco has built a "great firewall" in China or elsewhere confuse the provision of the basic pipes of the Internet, which include basic security features that every network must have, with more specific technological mechanisms which may be implemented to achieve the invasive effects that have raised specific concerns.

Some countries have chosen to restrict or limit access to information on the Internet based on political considerations, rather than on the freedoms that we enjoy in this country. While many have commented on the activities of the Chinese government in this regard, the issue is, in fact, global. Some Middle Eastern countries, for example, block sites critical of their leadership. And judicial action has been taken in France due to the failure of an operator to block local users' access to some types of information.

Cisco, however, has not and does not design products to accommodate political censorship. The tools built into our products that enable site filtering are the same the world over, whether sold to governments, companies or network operators. The features in our equipment are "off the shelf" and not altered in any way for any market or region. Similar technology is available from at least a dozen other US, Canadian, European and Chinese companies. Because of the threats to network operations that I previously mentioned, which exist around the world, there is no feasible way to manufacture equipment without these capabilities and it would not be desirable or sensible to do so. The management of information flow by a customer cannot be prevented by Cisco unless we are to also prevent the originally intended use of this technology, which would expose the Internet to the full risks of inevitable daily attacks. Networks attached to the Internet would literally stop working.

Cisco does, however, comply with all U.S. Government regulations which prohibit the sale of our products to certain destinations, or to certain users or to those who resell to prohibited users. We have not sold and do not sell our equipment to the countries listed on the U.S. Department of Treasury's OFAC (Office of Foreign Assets Control) list of embargoed nations, and we comply fully with all aspects of the Foreign Relations Authorization Act passed by Congress in the wake of Tiananmen Square.

More broadly, Cisco has played a leading role in helping to make Internet technology ubiquitous, allowing hundreds of millions of people in nearly every nation around the world to access information and ideas previously unavailable or inaccessible. Because our products are designed to expand the reach of communications systems, we build to open, global standards, and we vigorously oppose attempts by certain governments to balkanize the Internet by setting country-specific security requirements. We do not design custom or closed Internet systems. The Internet technology may not be perfect -- and the Internet itself can be misused -- but there has been no greater force in spreading

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00092 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.053

the power of ideas than the single worldwide Internet. The key to its growth and the flow of information it enables has been the standardization of one global network. This has been and remains the core of Cisco's mission.

For some, the Internet is a tool that liberates individuals from the constraints of time and distance, empowering those who previously had no access to the world's store of information. Some are fearful of this liberation as a mechanism for empowering non-state actors. Still others see the Internet as a tool used by governments to control content.

The policy response is complex. Among the questions that we have historically raised are: Has the Internet helped promote a dramatic increase in access to information in regions where content is nonetheless subject to certain limitations? Does active public engagement in such countries help to influence policy decisions? What policies will best help constrain political and other censorship contrary to First Amendment principles? If countries that engage in censorship are to be denied U.S. Internet technology, will those countries establish closed-standard Internets of their own to further restrict access to information?

To that end, policies that encourage governments to build their own Internets could be highly counter-productive by removing the leading platform for free expression. At the same time, Cisco sees benefit in the U.S. Government in making freedom of expression an integral part of its diplomacy. One means to do that that has been proposed is through the creation of an Office of Global Internet Freedom within the International Broadcasting Bureau. In doing so, the U.S. Government would be unambiguous about its intentions.

When the Internet first became a societal tool, it was largely available in western countries with broadly shared viewpoints about freedom of expression. It is inevitable as the Internet grows globally that there are differing viewpoints about its role in society. That has been true of every transformational technology, for example the television in the 20th Century.

Our challenge going forward is to ensure that as the Internet is globalized, we don't let it be balkanized in a way contrary to our goal of expanding its reach and liberating power.

Thank you for inviting us to appear before you today.

END

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00093 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.054

Statement of Senator Tom Coburn, M.D.

Hearing: "*Global Internet Freedom: Corporate Responsibility and the Rule of Law*"
Subcommittee on Human Rights and the Law
United States Senate Committee on the Judiciary
May 20, 2008

I would like to thank Senator Durbin for holding yet another compelling hearing on issues affecting human rights and the law. Senator Durbin and his staff are truly to be commended for their dedication to issues of such heavy import. This relatively new subcommittee has proven to be quite a force, introducing bipartisan legislation to address genocide, human trafficking, and child soldiers. These bills are already well on the way to bringing justice to victims of the most egregious human rights abuses. The Genocide Accountability Act has already been signed into law, the Child Soldiers Accountability Act passed the Senate by UC, and the Trafficking in Persons Accountability Act awaits consideration by the full Senate after receiving unanimous approval of the Senate Judiciary Committee.

This kind of progress is unusual in today's partisan atmosphere, but Senator Durbin has ensured success by reaching across the aisle to work together to tackle these issues. Under his leadership, we have approached every issue objectively, studying issues closely and talking to experts both at hearings and behind the scenes. In so doing, we have developed reasonable proposals to close gaps in current law that have inadvertently allowed the United States to serve as a safe haven for human rights perpetrators.

Today we address the issue of internet freedom. Nearly one and a half billion people now use the Internet, 220 million of which reside in China. This number has more than doubled since early 2006, when the House of Representatives first held a hearing on this issue. Such growth is explosive, and, amazingly, China now has the largest Internet population in the world. The introduction and widespread use of this technology in countries like China is one of the most exciting developments of our day. Information is power, and the more that Chinese citizens access that information, the more open their society will inevitably be.

Of course, nobody understands the power of the Internet better than the governments who seek to repress those societies. I have already mentioned China, but that country is not the only government with such pernicious censorship. According to Reporters Without Borders, at least 62 cyber-dissidents are currently imprisoned worldwide, while more than 2,600 Web sites, blogs or discussions forums were closed or made inaccessible in 2007. The group has identified

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00094 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.055

countries where internet freedoms are restricted, which are: China, Cuba, North Korea, Belarus, Myanmar, Egypt, Ethiopia, Iran, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, Vietnam and Zimbabwe. It named 11 additional countries as "countries under watch." It is my hope that today's hearing will shed light on how pervasive Internet censorship has become around the world.

This is not the first time Congress has addressed the issue of internet freedom. The House of Representatives, led by Congressman Chris Smith and the late Congressman Tom Lantos, held two recent hearings and have thereby created a thorough record for our benefit. I would like to thank my colleagues for their dedication to the issue and for the detailed groundwork they have already laid. The House hearings explored and established the factual record surrounding the relatively short history of American companies that have provided Internet service in countries where censorship is required by law. Those hearings examined in detail the steps and missteps of these companies as they began doing business in unfamiliar territory.

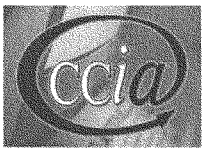
It is my hope that today we will tackle the challenge of discussing possible solutions for the problems that face these companies. While understanding the past is an important aspect of shaping solutions for the future, it is my hope that we can avoid re-litigating the same issues that have already been discussed at length. Our panel of witnesses, which includes industry experts and human rights advocates, should be able to explain the progress that has been made since the last hearing on this issue and answer questions that will help us better understand the challenge of preserving internet freedom around the world.

And while the focus of this hearing is worldwide, it is also my hope that while the eyes of the world are on China — in its response to the tragic earthquake and in anticipation of the summer Olympics — China's eyes are also on us, as we criticize government censorship of the Internet and call for more freedom for its citizens. I view this time as an opportunity to show the people of China what freedom looks like, and also to let the Chinese government know that its actions have not gone unnoticed. This is just another opportunity to lead by example, which is what I hope the American internet companies doing business in places like China will also choose to do. Their presence in these places is important, and it is crucial that they operate on the side of those seeking freedom, rather than oppression.

I look forward to the witnesses' testimony.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00095 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.056



900 17th Street, N.W.
Suite 1100
Washington, DC 20006
Phone: 202.783.0070
Fax: 202.783.0534
Web: www.ccianet.org

Computer & Communications Industry Association

Before the

Subcommittee on Human Rights and the Law
U.S. Senate Committee on the Judiciary

Regarding

Global Internet Freedom: Corporate Responsibility and the Rule of Law
May 20, 2008

Statement of
Computer & Communications Industry Association

The Computer & Communications Industry Association (CCIA) has been a longtime advocate of public policies that promote open markets, open systems, and open networks, and full, fair and open competition worldwide in the computer, telecommunications and Internet industries. We believe deeply in the free flow of information and ideas, and value the ability of the Internet to facilitate this flow. We commend Senator Durbin for convening this hearing on "Global Internet Freedom: Corporate Responsibility and the Rule of Law" before the Senate Judiciary Committee's Subcommittee on Human Rights and the Law, and we appreciate the opportunity for our views to be considered.

The Internet is often compared to the invention of the printing press in that it has broken down barriers to the mass sharing of information. The defining characteristic of the Internet is freedom: the free and unhindered flow of information over the Internet then enables and promotes the spread of political freedom around the world. Totalitarian regimes have historically depended on tightly controlling information, both domestic and from beyond their borders. They recognize that the more informed their people become, the more they will question the legitimacy and actions of their government. The Internet enables the widespread dissemination of information and ideas that pierce that control. Internet freedom is nothing less than freedom of expression in the 21st century. Any attempts to quash that freedom through censorship must be strongly opposed.

Yet certain governments such as the People's Republic of China have been engaging in such censorship. While China has experienced a meteoric rise through modernization and liberalization in the economic realm, the Communist Party shows no sign of loosening its control in the political realm. Chinese Internet censorship has consisted of technological suppression of information through the Great Firewall of China, and physical suppression through the arrest and detention of online writers. CCIA regrets that there have been past instances in which some U.S. high-tech companies have been forced

to accommodate such censorship. However, we must ask: is it fair to hold these companies solely to blame?

Our industry has been built on, and reaps the benefits of, the open nature of the Internet. U.S. companies only accommodate limits on that freedom when such limits are a prerequisite to operating in other nations, and only to the extent that is absolutely necessary. Moreover, our companies affirmatively seek to mitigate the scope of such limitations. The same cannot necessarily be said for the domestic market competitors of our companies.

The current situation is untenable in that it pits individual companies against powerful governments. Any individual company, no matter how large, cannot be expected to carry the banner of freedom alone in a conflict with governments, especially the government of the most populous nation on Earth.

Unfortunately, the Administration has squandered the opportunity to play an effective leadership role in protecting and promoting Internet freedom. While we appreciate the relatively recent creation and efforts of the Global Internet Freedom Task Force, we have not seen any concrete results. We recognize that U.S.-China relations are becoming increasingly complex. As our two nations grow ever more economically interdependent, contentious issues still abound and the relationship must be managed delicately. However, there is a need for greater engagement by the Administration on this issue. Is it wrong for U.S. companies to expect support from their government when they are being bullied and coerced by foreign governments? Surely, it is not for private companies to induce large-scale political and social reform, except by making new information services available to the maximum extent possible.

Such services can have a dramatic impact as seen in the aftermath of the devastating earthquake in Sichuan province. A Wall Street Journal article[1] last week discussed how "many are turning to technology instead of waiting for China's government to spread the news." The article also contrasted this response with "the paucity of information from Myanmar, where the government holds greater control over the Internet, and where the full extent of destruction wrought by Cyclone Nargis is still unknown." The information services our industry provides can make huge life-or-death differences, but cannot do so in the face of intense governmental opposition.

The magnitude of this issue necessitates the U.S. Government taking the lead and being a central player in promoting Internet freedom. Congress and the Administration must oppose the pressure being placed upon these businesses. As things stand now, it almost appears as if the U.S. Government prefers to play the "good cop" against China, leaving U.S. industry to wrestle with these difficult issues on its own. This strategy is neither fair nor effective. Our industry needs our Government to step up and be the bulwark of freedom and human rights in the online world.

---

[1] Mei Fong, "Earthquake in China: Technology Helped News Spread Quickly," *Wall Street Journal*, May 13, 2008

45688.058

Internet censorship has economic as well as political consequences. The success of e-commerce depends on users feeling comfortable and secure enough to utilize the services our industry provides. That comfort and security can only exist in an environment of Internet freedom. By engaging in Internet censorship, foreign governments are creating a hostile market environment and preventing their citizens from fully utilizing U.S. products and services. Some policymakers are realizing that Internet censorship can be a serious trade barrier that also keeps industry from realizing its market potential. The European Parliament recently passed such a proposal by an overwhelming majority. Here too, as an issue to be addressed in the context of trade negotiations and the WTO, it is clear that Internet censorship needs to be dealt with at the governmental level, not only the corporate level.

So long as the Administration does not do more to support U.S. Internet and other companies operating under repressive regimes, it is sacrificing Internet freedom to avoid making diplomatic waves. The U.S. Government should see our U.S. enterprises as allies rather than targets in the struggle for Internet freedom and human rights. We need to focus the combined efforts and resources of government and the private sector.

China regards this year's Beijing Olympics as an opportunity to showcase its economic and political power to the world. While China is eager to utilize the Internet to promote its successes, it seeks to close off the incoming flow of information from the outside world as well as prevent dissemination of inconvenient domestic occurrences. The U.S. must convince the Chinese government that the flow of information is not a one-way street, nor can it be selectively turned on and off. With the eyes of the world turned toward China, this is a period in which the Chinese government is unusually sensitive to, and therefore susceptible to, international public opinion. The U.S. Government must capitalize on this opportunity to secure a free and open Internet.

Our industry takes great pride in the fact that technology has greatly expanded the scope and freedom of social and political interaction. We do not want to see restrictions on an open Internet. However, even the most responsible public corporation has limited influence over matters of geopolitics, national diplomacy and international trade negotiations. Accordingly, CCIA calls on our government to support our industry by elevating freedom of the Internet to the top of our trade agenda, our human rights agenda, and our diplomatic agenda.

About CCIA:
CCIA is an international, nonprofit association of computer and communications industry firms, representing a broad cross section of the industry. CCIA is dedicated to preserving full, fair and open competition throughout our industry. Our members employ more than 600,000 workers and generate annual revenues in excess of $200 billion.

45688.059

Opening Statement of Senator Dick Durbin
Chairman, Subcommittee on Human Rights and the Law
Hearing on "Global Internet Freedom:
Corporate Responsibility and the Rule of Law"
May 20, 2008

Introduction

This hearing of the Judiciary Committee's Subcommittee on Human Rights and the Law will come to order.

The subject of this hearing is "Global Internet Freedom: Corporate Responsibility and the Rule of Law."

After a few opening remarks, I will recognize Senator Coburn, the Subcommittee's Ranking Member, for an opening statement, and then we will turn to our witnesses.

There is a tendency to view human rights solely as a foreign policy issue. In this Subcommittee, we have learned that is an inaccurate perception. Our world is growing smaller every day, a process accelerated by the internet revolution.

We have seen that human rights violations in other countries can affect the United States. To take just one example, this Subcommittee has discovered that over a thousand war criminals from other countries have found safe haven in the United States.

On the flip side, the actions of the U.S. government and U.S. companies affect human rights in other countries.

In future hearings, we will explore the impact of Corporate America on other fundamental human rights, but today we will focus specifically on the role of U.S. technology companies in internet freedom around the world.

Internet Freedom and Censorship

In 1791, the First Amendment of the Constitution was ratified, enshrining freedom of speech as the first fundamental right of all Americans. The First Amendment became an inspiration to people all over the world who yearn to throw off the yoke of oppression.

The year 2008 is the 60th anniversary of the Universal Declaration of Human Rights. After World War II, under Eleanor Roosevelt's leadership, the United States spearheaded the ratification of the Universal Declaration, which recognized freedom of expression as a fundamental right of all people.

The advent of the internet has allowed billions of people to exercise this right more fully.

45688.060

However, the internet is not free for everyone. Contrary to early predictions that the internet could not be controlled, many countries censor the internet and jail online dissidents.

In Egypt, blogger Kareem Amer is serving a four-year prison term for entries on his blog relating to Islam and President Hosni Mubarak. Just last month, 27-year-old Esra Abdel Fattah was arrested after forming a group online to protest the high price of food in Egypt. She was released only in return for her promise to give up internet activism.

In Cuba, citizens can be jailed for using the internet for "counter-revolutionary purposes." Cuban Telecommunications Minister Ramiro Valdes said in February 2007 that the Internet was a "tool for global extermination."

In Burma last fall, the military junta imposed a black out on the internet when images of Buddhist monks protesting the military's rule started appearing online.

In China, dozens of bloggers have been jailed, including Hu Jia, who was recently sentenced to 3½ years in prison based in part on online essays he wrote criticizing the Chinese government's human rights record.

Over 30,000 internet police monitor the web in China and the so-called "Great Firewall of China" prevents Chinese citizens from receiving accurate information about China's human-rights record in Tibet and Darfur, among many other subjects. Animated "internet police" pop up periodically to remind users that the internet is monitored.

The Role of American Companies

In today's hearing, we will examine the role that American companies play in internet censorship. At the outset, let me acknowledge the obvious: this is not a black-and-white issue.

U.S. technology companies face difficult challenges when dealing with repressive governments. However, these companies have a moral obligation to protect freedom of expression, a fundamental human right that has enabled them to make billions of dollars. There is no question that they have fallen short of the mark on more than one occasion.

Human rights groups have accused Cisco of providing networking equipment that forms the backbone of the Great Firewall of China and is used by other repressive countries to censor the internet and monitor users. I want to note that late last week the Subcommittee received some troubling information about Cisco's activities in China. This information has been shared with Cisco and we will discuss this further today.

Software produced by American companies such as Fortinet and Secure Computing has allegedly been used to censor the internet in Burma and Iran, respectively.

Google received significant public criticism when it decided to launch Google.cn, a China-specific search site that removes results to conform with China's censorship policies.

45688.061

At least 4 Chinese dissidents have been jailed based at least in part on information that Yahoo provided to the Chinese police.

Microsoft removes the blogs of internet activists from their blogging service in response to requests from repressive governments.

Internet Activism

Not all the news is negative, however. Around the world, internet activists are breaking down the walls of censorship. In Cuba, for example, students use flash drives, digital cameras, and clandestine internet connections to post blog entries and download information.

Yoani Sanchez, a Cuban blogger, poses as a tourist at internet cafes to make posts on her blog. She was recently named one of Time Magazine's most influential people of 2008.

Activists like Dr. Shiyu Zhou have also developed technology that allows users to break through firewalls and avoid censorship.

Three of our witnesses – Yahoo, Google, and Human Rights Watch – have been working for almost two years on developing a voluntary code of conduct for internet companies that do business in repressive countries. I look forward to hearing about the status of this long-awaited initiative. If American companies are unable to regulate themselves effectively, it may be time for Congress to step in.

Conclusion

As access to the internet continues to spread and change the way we inform and express ourselves, our government and American companies will be challenged to promote free speech and not to facilitate repression. With our collective efforts, perhaps someday the internet can fulfill its promise of empowering all people to exercise their right to seek information and express their opinions freely.

45688.062

Global Internet Freedom: Corporate Responsibility and the Rule of Law

Written Testimony of Arvind Ganesan
Director, Business and Human Rights Program, Human Rights Watch
To the Senate Committee on the Judiciary
Subcommittee on Human Rights and the Law

Tuesday, May 20, 2008

Mr. Chairman:

I welcome the opportunity to speak on the important matter of global internet freedom. I would also like to thank Senator Coburn, the ranking minority member of this Subcommittee. As someone who is from Oklahoma and whose family still lives there, I'm proud to say that my parents are thrilled at the prospect of delivering my testimony in front of one of their senators.

Human Rights Watch believes that the internet is a transformative force that can help open closed societies and provide the near-instantaneous flow of information to inform the public, mobilize for change, and ultimately hold institutions accountable. We have warned, however, that there is a real danger of a Virtual Curtain dividing the internet, much as the Iron Curtain did during the Cold War, because some governments fear the potential of the internet, want to control it and the companies that provide the services and products tied to it; and users fear the consequences of using it as a medium for openness and accountability.

Today, I would like to address three issues in relation to global internet freedom:

- The actions by some governments to restrict the flow of information and to punish individuals who exercise their right to free expression through this medium.

45688.063

- The ongoing efforts by industry, nongovernmental organizations (NGOs), academics, and financial institutions to press for self-regulation to ensure that leading companies who provide internet technologies and services are not complicit in abuses or forced by governments to capitulate to their repressive demands.

- The prospects for government-led change and opportunities to ensure respect for human rights, particularly in regard to companies.

Governments

In 2006, the human rights problems related to the internet in China came to light through Congressional hearings; reports by Human Rights Watch, Amnesty International, and other NGOs; and the press. Through those revelations, the public learned that the US company Yahoo! had provided user information to Chinese authorities that led to the imprisonment of online activists for years. We also learned that US companies, including Google, Microsoft, and Yahoo!, censor their search engines in China, in anticipation of what Chinese censors expect and in addition to what the Chinese government's firewall prohibits.

However, China is not the only government that actively tries to suppress its critics in the virtual world. Since 2006, there are other examples, both of activists being intimidated or silenced for their efforts and of restrictions that governments impose on the internet by controlling both providers and users:

- Just two weeks ago, on May 7, 2008, Egyptian officials beat Ahmed Maher Ibrahim, a 27-year-old civil engineer. His crime? He used Facebook to support calls for a general strike on May 4, President Mubarak's 80th birthday. Few people actually participated in the strike, but three days later, he was abducted by Egyptian officials in civilian clothes, beaten and insulted at New Cairo police station, then taken to the headquarters of the Interior Ministry's State Security Investigations (SSI) department where he was subjected to more beatings, and threatened that they would sodomize him with a broomstick. He was released without charges on the morning of May 8, but his captors asked him for the password to the Facebook group that he reportedly started, asked him about other participants in the group (whom he

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00103 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.064

did not know), and threatened to beat him even more severely the next time SSI detained him.

- In Russia, Saava Terentev, a musician in a town a little over 600 miles east of Moscow, is being tried as an "extremist" because he spoke out about corruption in Russian law enforcement after reading a newspaper story about a newspaper being harassed by the authorities for reporting on corruption. He issued a harsh critique of corrupt police in a blog posting and an extremely offensive, but clearly ironic, "modest proposal" that they be burned in the public square. It was shortly deleted by the blog's owner, but now the authorities are prosecuting him for his sarcastic rant. We believe that this is the Russian government's first test case to try to use a law to restrict free speech on the internet. Additionally, the government has promulgated a decree that allows unfettered surveillance of the internet and other communications mediums without telling the user or the provider. But they do require the provider (potentially companies) to pay for the surveillance equipment. There are also some troubling proposals that are being circulated in the Duma. One is to regulate websites that receive more than 1,000 hits a day. Another is to separate the Russian internet from the rest of the world, along the lines of the Chinese firewall, so that the government could monitor content and shut down the link between the Russian internet and the rest of the world. Between those efforts and the attempts to go after bloggers it appears that the internet, which is perhaps one of the few open forums left in Russia, is now falling under government control.

- During its crackdown, following protests by monks, Burma's military junta shut down the country's internet connections to make sure no information got into the country and more importantly, that little information got out of the country. In total, the OpenNet initiative found that the junta blocked about 85 percent of e-mail service providers and virtually all of political opposition and pro-democracy sites. Then, in late September 2007, the government apparently disconnected the main telecommunications lines in two cities to stop the flow of information. Some bloggers, however, used satellite and cellphone services. This is a chilling example of how far certain governments will go to stop the flow of information.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00104 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.065

- The government of Syria regularly restricts the flow of information on the internet and will arrest individuals who post comments that the government deems too critical. Internet use in the country has exploded in the last few years and could be a crucial medium for the flow of information. However, Human Rights Watch has documented at least five cases since 2005 in which the government has arrested individuals because they posted comments critical of the government online, sent critical e-mails, or posted other information on the web. For example, on June 30, 2007, military intelligence arrested Tarek Biasi because he "went online and insulted security services." He was held incommunicado by the authorities and then sentenced to three years imprisonment on May 11, 2008, for "diminishing national feeling" and "weakening the national ethos." These are not the government's only tactics. Security services often force internet café owners to spy on their customers. In one case, an internet café owner filmed a customer who was sending comments and information to opposition websites outside of the country. On July 25, 2007, the government promulgated regulations that required all website owners to display the name and e-mail of the author of any article or comment on their website. This brazen regulation is clearly intended to chill critical speech by making it easier for the government to identify its critics online, particularly as anonymous postings have become a crucial means for individuals to avoid surveillance, or worse. Finally, the government also blocks websites, most notably those that are critical of the government, such as Arabic opposition newspapers' websites outside of the country.

These are just some of the cases around the world in which governments try to restrict the internet and silence users. What is clear is that government efforts to control the internet have multiplied around the world. While China has in many ways become the poster child for our efforts to stop censorship abuses, for other repressive governments such as those I have mentioned, China provides a model to be replicated. If that model is the ideal for internet repression, then the role of companies cannot be overlooked since they are clearly part of the Chinese government's efforts to censor the internet and obtain user information. As we have previously documented, Microsoft, Google, and Yahoo! censor their search engines in anticipation of what the Chinese government expects. Blogs have been shut down, and user information has been turned over to the government.

4

45688.086

A Voluntary Code of Conduct

On January 17, 2007, leading companies including Yahoo!, Microsoft, Google, Vodafone, French Telcom, and Telia Senoria, along with human rights organizations (including Human Rights Watch, Amnesty International, Human Rights First, the Committee to Protect Journalists, Human Rights in China, Reporters without Borders, and the World Press Freedom Association), socially responsible investors, and academics, started on a process to develop a voluntary code of conduct and process of enforcement to try to curtail censorship and protect user information. We believe a system with three critical features could make a real difference in many censoring countries. These features are: a strong but reasonable code of conduct, an effective but not overly bureaucratic governance process, and independent monitoring of companies that sign on to ensure they actually take steps to curtail censorship and protect their users. Now, almost 18 months later, it would be great to tell you that a code is finalized and a system is in place to address these problems, but instead, we are still negotiating, and in the meantime, internet users are no safer, and censorship continues.

Not every company is in the same place nor is it fair to say companies don't care about human rights. After a high profile lawsuit by the families of jailed cyber dissidents, Yahoo! settled and has set up a fund to help cyberdissidents obtain legal aid. Google has used technologies like Google Earth to monitor some of the world's worst human rights crises, such as Darfur.

However, as laudable as those efforts might be, they do not address steps companies should take to ensure that their operations do not contribute to violations of human rights, such as censorship or the persecution of cyberdissidents. Some companies have been more aggressive, especially those that have faced the most controversy. Yahoo! has raised these issues with the Secretary of State, and some companies, such as Microsoft, have become more rigorous about censorship and the circumstances under which they will take down blogs.

Much more remains to be done. While companies have developed differently in regards to their human rights procedures, a voluntary industry initiative is only as strong as its weakest link. Without disclosing the details of discussions that are under the Chatham House rules, I can say that a fundamental problem is that some companies continue to be very resistant to the idea of independent monitoring, in particular to a system that would allow for an independent third party to assess: 1) whether companies have put

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00106 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.067

policies into place that demonstrate a respect for freedom of expression and user privacy; 2) that those polices are diligently implemented; and 3) that their implementation is effective in curtailing these human rights problems. Unfortunately, we do not have such a system. Right now, the preferred option for companies is a system in which they will decide who the monitors are and what they will see, while companies implement those standards at a pace convenient to them.

In other words, companies will express support for human rights but also ask the public to basically trust them to do the right thing. There are several problems with that approach. First, this is exactly the situation that led to the problems we are trying to solve. Companies have already been opaque and exercised discretion over their actions, and to claim that the same approach will change things is dubious. For example, in China, Google and others choose what to censor. Even though Google and other companies now provide a disclaimer to notify users that censorship occurs, they still decide what to censor and whether they will even challenge the government's actions.

Second, it is difficult to point to a company within the voluntary standards process that has robust human rights policies and procedures in place more than two years after the problems in China were disclosed. Google, for example, has actively resisted such efforts. On May 8, Google's board voted down two shareholder proposals, including one sponsored by Amnesty International and the NYC Pension Funds, calling on the company to implement policies and procedures to protect human rights and another calling for a board committee on human rights. Sergey Brin, the company's co-founder, abstained from the vote and expressed support for human rights, but felt these proposals were not the appropriate way to approach the issue. What he did say was, "I think it makes sense to have a separate, a group of independent people in Google who meet regularly to discuss [these issues]." Frankly, that is not good enough.

Google's resistant stance and the lack of consensus on voluntary standards raise a fundamental question: What is holding up these corporations from finding an effective means of protecting user privacy and curtailing censorship? It can't be technical or technological challenges because industries like pharmaceuticals are very complex yet regulated. And in the case of internet companies, nobody is calling for a massive new bureaucracy like those that regulate other industries, just an agreement to be independently monitored.

6

45688.088

Mr. Brin also recently defended Google's activities in China. "Google has a far superior track record than other search companies with respect to making information freely available," he said. This is a bold statement, but on what basis is he making it and what assurance is Google giving to the public to support this claim? Without some form of independent assessment of their activities, assertions like this simply are not credible.

A key purpose of our joint voluntary initiative is to provide the public with real assurance so that they can have confidence in companies or an industry that claims to oppose censorship and respect user privacy. After all, it will be the public and users who are the victims of censorship and whose information may be turned over to authorities. But that assurance is unlikely without meaningful oversight. A useful analogy is that of airlines. We would not accept that the best way to monitor airline safety is to allow airlines to do it themselves. Instead, we insist that someone else oversee them and are rightly critical of both the airlines and the monitors if they fall down on the job. Independent oversight is a critical component in protecting the public interest and it should be in the case of protecting freedom of expression and user privacy. Independent oversight is especially important with a medium and technologies that have the power to open societies, and because companies have already shown that they cannot or will not do it themselves.

Government Intervention

While we hope and plan to work towards an effective voluntary standard, it is unlikely that voluntary initiatives alone will be sufficient. A voluntary initiative will not apply to companies that do not join and it is difficult to see how it will get effectively implemented in countries where the government is very good at dividing and pressuring companies to capitulate to its demands, sometimes in exchange for access to a lucrative market. And most importantly, a voluntary initiative may be least effective in curtailing governments' efforts to obtain user information about cyberdissidents from companies, because a voluntary effort is not sufficient to stand up against the pressures a government can assert against companies.

For those and other reasons, we believe a regulatory approach is a necessary complement to a voluntary initiative. It would help to ensure that the playing field is level for human rights since rules would apply to far more companies than those who join a voluntary initiative; that there are meaningful consequences for companies who do not respect those standards; it would make it more difficult for governments to force companies into becoming complicit in human rights abuses; and could encourage a

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00108 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.089

more assertive US foreign policy on these issues. There have been proposals circulating in Congress and one is in the House. We believe that any regulation should, at a minimum, contain the following elements:

- A requirement that companies have effective policies and procedures in place to safeguard human rights modeled after provisions in the US Foreign Corrupt Practices Act.
- A provision that requires companies to catalog and record efforts by governments to censor information.
- A process in which foreign government requests for user information can be referred to US diplomatic channels so that a company and its personnel are at less risk of pressure or retaliation.
- A requirement that companies locate personal information outside of jurisdictions that punish individuals exercising their right to free expression where the authorities may try to obtain personal data to do so.
- A private right of action so that victims can seek redress against companies that violate their rights.
- Clear and aggressive steps that the US government should take to combat censorship and protect user privacy through its foreign policy, trade policy, and other means.
- An examination of whether certain types of hardware and software, such as servers and other equipment, should be subject to export controls because of their capacity to be used by governments to spy on individuals and censor information.
- Effective penalties to deter companies from violating human rights.
- Restricting access to federal funds for companies that do not abide by these standards.

A useful model for this approach is the Foreign Corrupt Practices Act (FCPA). That act allows for companies to face penalties if they do not have adequate systems in place to prevent bribery as well as penalties if they actually engage in corruption. That approach could work quite well in regards to the internet and would easily complement a voluntary initiative since it would require a company to put systems into place to prevent abuses and would also hold it accountable were the company party to abuses. The FCPA also disproves the notion that regulations intended to protect the public good limit companies' ability to do business. The FCPA has been in force for more than 30 years

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00109 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.070

and US business is still thriving abroad. Indeed, Microsoft, Google, and Yahoo! did not even exist when the act was passed, yet they seem to be doing reasonably well.

Companies have said that they might support regulation in theory, but seem to oppose existing efforts. Much like human rights policies and a voluntary initiative, they support them in principle, but apparently, not in practice. It would be helpful to understand how the companies and the industry intend to move forward effectively and credibly in terms of voluntary and mandatory standards. I would welcome the opportunity to come before you again or at regular intervals to report on such progress and would hope that the other witnesses today would do the same.

Thank you again for this opportunity to speak on this important subject.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00110 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.071

Statement for the Record of Leslie Harris
President/CEO, Center for Democracy & Technology

Before the Senate Judiciary Committee,
Subcommittee on Human Rights and the Law

"Global Internet Freedom: Corporate Responsibility and the Rule of Law"
May 20, 2008

Chairman Durbin and Members of the Subcommittee:

The Center for Democracy & Technology ("CDT") applauds the Subcommittee's leadership in addressing the growing threat of state-sponsored censorship and surveillance of the Internet, and we appreciate the opportunity to submit this written testimony.

CDT's core mission is to advocate for public policies, standards and industry practices that keep the Internet open, innovative and free. We believe that an open Internet can be a powerful tool for human rights and democracy. It can facilitate government accountability and transparency, allowing citizens to pierce through official propaganda and access vast alternative sources of information. The Internet is a uniquely decentralized "end to end" network, which places power in the hands of users rather than with gatekeepers in the middle. It permits anyone with a connection to speak, advocate for political freedom and collaborate with others. It has been 60 years since the Universal Declaration of Human Rights first articulated a broad right to freedom of expression regardless of borders.[1] The Internet offers a unique promise to fulfill that vision.

Because of its openness and low barriers to entry, the Internet is a uniquely disruptive technology to repressive regimes and its global deployment presents an unprecedented challenge to governments that seek to tightly control the flow of ideas and information within their borders.

[1] Article 19, Universal Declaration of Human Rights (1948), http://www.un.org/Overview/rights.html.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00111 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.072

Trade liberalization and the lure of the global markets have made participation in the global Internet an imperative even for many repressive governments. The challenge as they see it is to harness the Internet's power for economic growth while limiting its freedoms.[2]

The task of controlling such a highly distributed network is not an easy one. As the numbers of users increase along with the sheer number of devices that connect to the Internet, the ability to control what people do and see online diminishes and the threat to totalitarian governments escalates. Some countries, including China, have responded with an elaborate censorship and surveillance apparatus,[3] while other governments simply encourage citizens' self-censorship by spreading *rumors* of the existence of such monitoring.[4] In other countries, Internet access itself is limited or banned outright.[5]

Increasingly, repressive regimes are turning to Internet companies and other technology intermediaries to assist with censorship and surveillance. Global technology companies are increasingly faced with a Hobson's choice: follow the law of the countries in which they offer services and risk participating in human rights violations, or refuse to cooperate and risk loss of a business license and the right to provide services in that country. In CDT's view, neither result serves the goal of Internet freedom.

While there is no easy answer to the rise of Internet repression, we strongly believe that the United States government must play a decisive role and use the instruments at its disposal

---

[2] China, for example, wants the economic growth and world recognition that comes with hosting the Olympics but refuses to grant the media and Internet freedom that should rightly accompany it. *See* Ben Blanchard, "China won't guarantee Web freedom over Olympics," *Reuters* (May 8, 2008) http://www.reuters.com/article/reutersComService_2_MOLT/idUSPEK14583520080508.

[3] *See, generally*, Human Rights in China, http://www.hrichina.org/public/. *See also* OpenNet Initiative's China profile: http://opennet.net/research/profiles/china.

[4] *See* OpenNet Initiative's discussion of "induced self-censorship": http://opennet.net/about-filtering.

[5] *See, e.g.*, the OpenNet Initiative's analysis of the Burmese government's shut down of the Internet during fall 2007 following massive protests: "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma," http://opennet.net/research/bulletins/013.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00112 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.073

including diplomacy, trade policy, and foreign aid to advocate for Internet freedom. We further urge the U.S. government to work collaboratively with U.S. technology companies to help them better identify and manage the risks posed by providing Internet services or selling sensitive technologies in high-risk countries.

Companies, too, have a duty to take actions that protect the free expression and privacy rights of their users. Companies must engage in rigorous due diligence and risk assessment when entering difficult markets to identify human rights risks and integrate the protection of human rights into all relevant aspects of their operations. As we discuss further below, CDT also believes that an accountable set of voluntary industry principles can help companies chart an ethical path forward and resist abusive censorship and surveillance demands by governments.

➤ **Congress and the Executive Branch should make global Internet freedom a top human rights and foreign policy priority.**

Congress has an important role to play in ensuring that Internet freedom is fully incorporated into United States human rights and foreign policy and that it is a central focus of diplomacy, trade and foreign aid. Especially where, as in the case of Internet freedom, many countries are failing to live up to their human rights obligations, the United States and other democratic nations have a duty to act.[6] Both Congress and the Executive Branch should make Internet freedom a top human rights and foreign policy priority. The State Department should monitor and report on threats to Internet freedom and should fully incorporate the issue into its diplomatic efforts in all relevant forums.

Congress should also consider how progress toward Internet freedom could be factored

[6] It is important to note that the United States has ratified or signed key human rights treaties, including the International Covenant on Civil & Political Rights, http://www.unhchr.ch/tbs/doc.nsf/newhvstatusbycountry?OpenView&Start=1&Count=250&Expand=187#187

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00113 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.074

into the criteria for development assistance and the conditions for new trade agreements.[7] We believe that Internet censorship should be treated as a trade barrier in appropriate circumstances – initial steps have been taken in the European Union toward adoption of this approach and it has been discussed in U.S. policy circles.[8] It is also appropriate for Congress to direct that there be an examination of whether narrowly targeted export restrictions are necessary when technology, equipment or expertise is specifically designed for surveillance or censorship.[9]

Finally, we strongly support the statutory creation of an Office of Global Internet Freedom in the Department of State, which would serve as the focal point for mobilizing the tools of U.S. diplomacy and policy in furtherance of online freedom of expression and privacy, and which would institutionalize and continue the work of the Global Internet Freedom Task Force (GIFT) created by the State Department in 2006.[10]

The steps that we outline are simple and straightforward, but achieving them may be easier said than done. There is considerable "policy incoherence" between the United States'

---

[7] For example, the Foreign Assistance Act could be amended to include Internet freedom as an explicit factor to be considered when allocating development assistance. *See* 22 U.S.C. § 2151n(c). Additionally, Congress annually appropriates money to help fund the Millennium Challenge Account, managed by the President's Millennium Challenge Corporation, and could ensure that these funds are used to advance Internet freedom in country grantees. For Fiscal Year 2008, while "freedom of expression" is a factor in both the Civil Liberties Indicator and the Voice and Accountability Indicator, Internet freedom – both online freedom of expression and privacy of digitized personal information – are not explicit factors: *Guide to the MCC Indicators and Selection Process, Fiscal Year 2008*, http://www.mcc.gov/documents/mcc-fy08-guidetoindicatorsandtheselectionprocess.pdf.

[8] *See* Eric Bangeman, "EU may begin treating 'Net censorship as a trade barrier," *Ars Technica* (Feb. 27, 2008), http://arstechnica.com/news.ars/post/20080227-eu-may-begin-treating-net-censorship-as-a-trade-barrier.html. *See also* "A Framework for Global Electronic Commerce" (July 1997), http://www.w3.org/TR/NOTE-framework-970706.html#content.

[9] *See, e.g,* Keith Bradsher, "At Trade Show, China's Police Shop for the West's Latest," *New York Times* (April 26, 2008) (noting that the Commerce Department's crime control export regulations "paid little attention to the rising computer industry and have not been updated."), http://www.nytimes.com/2008/04/26/business/worldbusiness/26security.html. *See also* Naomi Klein, "China's All-Seeing Eye: With the help of U.S. defense contractors, China is building the prototype for a high-tech police state. It is ready for export," *Rolling Stone* (May 29, 2008), http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye/.

[10] http://www.state.gov/g/drl/rls/78340.htm.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00114 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.075

positions on human rights and its policies on trade and foreign aid.[11] For example, the U.S. government has conferred "most-favored nation" trade status on countries such as China and Vietnam,[12] which have poor human rights records and engage in pervasive Internet surveillance and censorship. The U.S. government also provides significant aid to countries that are key allies in the "war on terrorism" such as Pakistan[13] and Egypt,[14] but that also have poor human rights records and spotty records on Internet freedom. If Congress decides to elevate the importance of Internet freedom in foreign policy and trade (as we think it should), then it will be critical that such mandates be implemented in a manner that is even-handed and coherent.

Furthermore, the United States and other democratic countries must show their commitment to Internet freedom by carefully guarding Internet freedom at home. Democratic countries have been increasingly turning to content blocking and other Internet speech

---

[11] The UN Special Representative on business and human rights provides a useful discussion of "horizontal policy incoherence" where a government's policies on such things as "trade, investment promotion, development, [and] foreign affairs – work at cross purposes with stated human rights policies and obligations and the agencies charged with implementing them." John Ruggie, *Protect, Respect and Remedy: a Framework for Business and Human Rights*, at 11-14 (April 7, 2008), http://www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf.

[12] George W. Bush, Normal Trade Relations Treatment Executive Order [China] (Dec. 27, 2001), http://www.whitehouse.gov/news/releases/2001/12/20011227-1.html; Proclamation To Extend Nondiscriminatory Treatment (Normal Trade Relations Treatment) to the Products of Vietnam (Dec. 29, 2006), http://www.whitehouse.gov/news/releases/2006/12/20061229-7.html.

[13] According to Reporters Without Borders, "The United States has given the Pakistani intelligence services much technological help to monitor online traffic and it has played a major role in arresting terrorists," http://www.rsf.org/article.php3?id_article=10794. *See also* David Rohde, et al., "U.S. Officials See Waste in Billions Sent to Pakistan," *New York Times* (Dec. 24, 2007), http://www.nytimes.com/2007/12/24/world/asia/24military.html?ex=1356152400&en=19a8b44eb685fafa&ei=5088&partner=rssnyt&emc=rss. *See also* OpenNet Initiative's report on Pakistan's Internet filtering: http://opennet.net/research/profiles/pakistan.

[14] *See, e.g.*, Issandr El Amrani, "Cashing in on the war on terrorism: In exchange for its support since Sept. 11, Egypt has received billions in international aid and diminished scrutiny of its human rights abuses," *Salon.com* (Feb. 13, 2002), http://dir.salon.com/story/news/feature/2002/02/13/egypt/. *See also* "Egypt blogger jailed for 'insult'," *BBC News* (Feb. 22, 2007), http://news.bbc.co.uk/2/hi/middle_east/6385849.stm; Ellen Knickmeyer, "Fledgling Rebellion on Facebook Is Struck Down by Force in Egypt," *Washington Post* (May 18, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/05/17/AR2008051702672.html.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00115 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.076

restrictions, for example, to address social ills.[15] Moreover, since 9/11, both the U.S. and Western Europe have taken steps that make it easier to spy on the activities of Internet users and access personal information, setting a poor example that repressive countries are quick to cite in support of their own surveillance.[16] While it is not our intention here to debate the merits of particular U.S. domestic policies, there is little doubt that activities such as the NSA's illegal warrantless wiretapping of Americans' electronic communications and the alleged involvement of U.S. companies in that effort have weakened our position as the standard bearer of Internet freedom.[17]

➤ **The technology industry must exercise due diligence in order to minimize human rights risk.**

As the global technology industry pursues new markets, it is increasingly confronted with government demands to censor Internet content and turn over information on users in circumstances that place human rights at risk. Most often, these activities are a condition of doing business in a country. Companies have struggled to find an ethical path forward, sometimes pushing back or finding ways to skirt the edges of vague censorship mandates in

---

[15] *See* OpenNet Initiative's analysis of North America's and Europe's voluntary and legally mandated restrictions on Internet speech: http://opennet.net/research/regions/namerica; http://opennet.net/research/regions/europe.

[16] For example, there has been an ongoing battle in Congress over whether to legitimize NSA warrantless wiretapping of Americans' electronic communications and immunize the complicit telecommunications companies. *See* House Judiciary Committee hearing on Sept. 5, 2007: http://judiciary.house.gov/oversight.aspx?ID=367, and Sept. 18, 2007: http://judiciary.house.gov/oversight.aspx?ID=370; and Senate Judiciary Committee hearing on Oct. 31, 2007: http://judiciary.senate.gov/hearing.cfm?id=3009. Also, the Justice Department has sought to expand the Communications Assistance for Law Enforcement Act ("CALEA") to reach the Internet, and thereby impose burdensome surveillance technology mandates onto online service providers. *See American Council on Education v. Federal Communications Commission*, 451 F.3d 226 (D.C. Cir. 2006). Similarly, the European Union and Western European countries have been stepping up surveillance capabilities and have imposed new requirements for data retention. *See, e.g.*, "German court allows limited Internet surveillance," *AFP* (Feb. 27, 2008), http://afp.google.com/article/ALeqM5h3zO5qr1MexZtdmJMTdQTVsQVjcg; and the EU's directive on data retention (March 15, 2006): http://register.consilium.europa.eu/pdf/en/05/st03/st03677-re12.en05.pdf.

[17] *See* "The Slippery Slope of Web Censorship," *ABCNews.com* (Oct. 25, 2007), http://abcnews.go.com/Technology/story?id=3771510&page=1.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00116 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.077

order to make more information available to users, and other times stumbling badly and inadvertently facilitating human rights violations.[18] While some argue that technology companies should simply withdraw from challenging markets, most Internet freedom advocates agree with CDT that the presence of the U.S. Internet industry – and the communications and information services they provide – plays an important role in expanding global Internet freedom.

Having said that, the question remains: *What should be the obligations of these companies with respect to human rights and how should those obligations be effectuated?* There is little doubt that companies are also human rights actors. As the UN special representative on business and human rights has concluded, while "their responsibilities cannot and should not mirror the duties of States," companies do have an obligation to respect human rights – and that duty is not "passive" but rather must entail "positive steps."[19] The UN special representative on business and human rights, John Ruggie, set forth a thoughtful framework for corporate action and public policy that centers on the exercise of "due diligence" and the identification and management of human rights risk. As Ruggie explains, the corporate responsibility to respect human rights must be embraced at the highest levels of a company and must be incorporated into all aspects of operations. "Due diligence," specifically, requires:

- Rigorous identification of human rights risks posed by a country context, the company's activities within that context, and the activities of its business partners and suppliers;
- Development and implementation of a proactive plan to minimize or eliminate human rights risks; and
- Ongoing monitoring and auditing to track performance and refine practices.[20]

---

[18] *See* Human Rights Watch, *Race to the Bottom: Corporate Complicity in Chinese Internet Censorship* (Aug. 2006), http://www.hrw.org/reports/2006/china0806/china0806web.pdf.

[19] Ruggie report, *supra* note 11, at 16-17.

[20] Ruggie report, *supra* note 11, at 17-19. Similarly, the London-based International Business Leaders Forum (IBLF) has created a comprehensive human rights risk assessment model, with eight discreet steps companies

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00117 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.078

The due diligence approach outlined in the Ruggie report will not produce binary rules that apply to all companies in all circumstances nor will it ensure that mistakes will never occur. The technology sector will continue to have to navigate between the demands of domestic law and their obligation to respect human rights. But the sector will be better equipped to make responsible decisions about which products and services should be offered in a particular market and to build in safeguards for respecting human rights into all aspects of their operations.

➤ **The technology industry should adopt voluntary principles to guide its conduct.**

While it is incumbent on each company facing demands for abusive filtering and surveillance to engage in due diligence as described above, CDT strongly believes that collective action will strengthen individual company efforts. In our view, the most promising path forward is a set of robust voluntary industry principles, developed in concert with human rights groups and other key stakeholders, and widely adopted as a global industry standard.

For the past 18 months, CDT has had the privilege of co-facilitating an important multi-stakeholder initiative to develop voluntary principles to guide the Internet and telecommunications industry response to the growing challenges to online free expression and privacy. Both U.S. and European companies have been participating, as have major human rights and press freedom groups, leading academic institutions and social investment funds.[21]

By agreement of all parties, the process has been highly confidential in order to build trust and encourage a candid exchange of ideas and information. For that reason, I cannot discuss the substance of the principles or the supporting accountability and governance documents, all of

---

should take, which has been "road-tested" over the past year, http://www.iblf.org/resources/general.jsp?id=123946.

[21] *See* CDT-BSR press release announcing multi-stakeholder principles initiative (Jan. 18, 2007): http://www.cdt.org/press/20070118press-humanrights.php.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00118 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.079

which are in draft form. I can say, however, that this process has been taken very seriously by all participants and has already led to new thinking and practices among some of the companies involved. And while there are still important issues to resolve, I am hopeful that we are close to reaching our goal. If we succeed, I am confident that the results will begin to provide an ethical and accountable path forward for the companies at the table, arming them to better respond to human rights challenges. I am also hopeful that we will sow the seeds of a global industry standard and create a powerful forum for shared learning and collaborative action between the companies and other stakeholders, including like-minded governments.

Conclusion

If Congress believes that legislation is warranted, there are steps it can take to support the wider adoption of industry principles and ensure that U.S. companies are better equipped to respect human rights when operating in risky markets, such as:

- Encouraging companies to assess and better manage human rights risks associated with the provision of Internet products and services in repressive countries;
- Harnessing the knowledge and resources of the United States government to support better company decision-making when faced with challenges to free expression and privacy; and,
- Encouraging participation in relevant voluntary corporate social responsibility initiatives.[22]

In sum, the challenges to global Internet freedom cannot be addressed by either government or industry alone. The U.S. government must leverage the powerful instruments of diplomacy, trade, and foreign aid in the service of Internet freedom, and companies must accept their obligations as human rights actors and exercise due diligence when facing free expression and privacy challenges in difficult markets. Collective action to develop industry principles is key as

[22] CDT is not convinced that proposals like Title II of the Global Online Freedom Act in the House [H.R. 275] (110th Congress), which place the U.S. government in an adversarial relationship with U.S. businesses, is either workable or wise. CDT recently wrote an analysis of GOFA (May 2, 2008): http://www.cdt.org/international/censorship/20080505gofa.pdf.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00119 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.080

is greater collaboration between government and industry.

CDT looks forward to working with Congress on ways to advance global Internet freedom.

###

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00120 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.081

New York Times

November 10, 2008

Internet Attacks Grow More Potent

By JOHN MARKOFF

SAN FRANCISCO — Attackers bent on shutting down large Web sites — even the operators that run the backbone of the Internet — are arming themselves with what are effectively vast digital fire hoses capable of overwhelming the world's largest networks, according to a new report on online security.

In these attacks, computer networks are hijacked to form so-called botnets that spray random packets of data in huge streams over the Internet. The deluge of data is meant to bring down Web sites and entire corporate networks. Known as distributed denial of service, or D.D.O.S., attacks, such cyberweapons are now routinely used during political and military conflicts, as in Estonia in 2007 during a political fight with Russia, and in the Georgian-Russian war last summer. Such attacks are also being used in blackmail schemes and political conflicts, as well as for general malicious mischief.

A survey of 70 of the largest Internet operators in North America, South America, Europe and Asia found that malicious attacks were rising sharply and that the individual attacks were growing more powerful and sophisticated, according to the Worldwide Infrastructure Security Report. This report is produced annually by Arbor Networks, a company in Lexington, Mass., that provides tools for monitoring the performance of networks.

The report, which will be released Tuesday, shows that the largest attacks have grown steadily in size to over 40 gigabits, from less than half a megabit, over the last seven years. The largest network connections generally available today carry 10 gigabits of data, meaning that they can be overwhelmed by the most powerful attackers.

The Arbor Networks researchers said a 40-gigabit attack took place this year when two rival criminal cybergangs began quarreling over control of an online Ponzi scheme. "This was, initially, criminal-on-criminal crime though obviously

the greatest damage was inflicted on the infrastructure used by the criminals," the network operator wrote in a note on the attack.

The attack employed a method called reflective amplification, which allowed a relatively small number of attack computers to generate a huge stream of data toward a victim. The technique has been in use since 2006.

"We're definitely seeing more targeted attacks toward e-commerce sites," said Danny McPherson, chief security officer for Arbor Networks. "Most enterprises are connected to the Internet with a one-gigabit connection or less. Even a two-gigabit D.D.O.S. attack will take them offline."

Large network operators that run the backbone of the Internet have tried to avoid the problem by building excess capacity into their networks, said Edward G. Amoroso, the chief security officer of AT&T. He likened the approach to a large shock absorber, but said he still worried about the growing scale of the attacks.

"We have a big shock absorber," he said. "It works, but it's not going to work if there's some Pearl Harbor event."

Over all, the operators reported they were growing more able to respond to D.D.O.S. attacks because of improved collaboration among service providers.

According to the Arbor Networks report, the network operators said the largest botnets — which in some cases encompass millions of "zombie" computers — continue to "outpace containment efforts and infrastructure investment."

Despite a drastic increase in the number of attacks, the percentage referred to law enforcement authorities declined. The report said 58 percent of the Internet service providers had referred no instances to law enforcement in the last 12 months. When asked why there were so few referrals, 29 percent said law enforcement had limited capabilities, 26 percent said they expected their customers to report illegal activities and 17 percent said there was "little or no utility" in reporting attacks.

45688.083

Written Statement of:

John G. Palfrey, Jr.
Clinical Professor of Law & Executive Director
Berkman Center for Internet & Society, Harvard Law School
with
Colin Maclay
Managing Director
Berkman Center for Internet & Society, Harvard Law School
May 20, 2008

Mister Chairman, distinguished members of the committee:

I would like to offer my deep appreciation for the Committee's interest in this important matter. Congressional engagement is an important factor in deepening understanding of the nexus between global Internet freedom and corporate responsibility, and an essential element for ensuring that the Internet continues on its path towards becoming an ever-greater force for democratic participation and human rights advancement worldwide.

My name is John Palfrey. I teach Internet law at Harvard Law School. My primary research interest is in examining issues related to the Internet and democracy. I am also Executive Director of the Berkman Center for Internet and Society. Of relevance to this hearing, I am a Principal Investigator of the OpenNet Initiative (ONI), a project based at the University of Toronto, the University of Cambridge, the Oxford Internet Institute, and Harvard Law School, that has been conducting research and analysis of Internet censorship, filtering, and surveillance practices worldwide. I submit this testimony along with my colleague, Colin Maclay, Managing Director of the Berkman Center. Together with other great colleagues at Berkman, we have spent more than two years on a multi-stakeholder effort—involving businesses, non-profits, socially responsible investors, and academics—to develop principles and associated implementation measures for technology companies seeking to protect and advance privacy and free expression worldwide.

The strides made through this initiative—engaging a range of parties, deepening understanding of the complexity of the issues for each stakeholder, and working towards a viable solution—have been encouraging. I urge you to support this process, in lieu of strong legislation at this time. As this testimony demonstrates, due to the dynamic nature of the ICT sector and the complexities of the existing regulatory environment, legal regimes cannot yet adequately address the dilemmas posed by the rise of global filtering, censorship, and surveillance practices worldwide, and are unlikely to be capable of doing so in the near term.[1] Furthermore, the proposals currently being considered could be harmful, potentially forcing organizations out of foreign countries altogether, by

[1] John G., Palfrey, "Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet" GLOBAL INFORMATION TECHNOLOGY REPORT, p. 69, World Economic Forum, 2006-2007. Available at SSRN: http://ssrn.com/abstract=978507

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00123 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.094

requiring them to break local laws and by limiting their capacity for constructive engagement. It would be premature to act now with blunt legislation, as we do not yet know the most effective and sustainable ways for companies to meet these complex challenges. Rather, there are several activities which the US government could support and contribute to, including: proactive policy engagement, multi-stakeholder input, learning, and commitment, technological innovation, formalized relations with companies around these issues, and user empowerment, that could have immediate impact not only on our understanding of the landscape, but on our ability to positively contribute to protecting the human rights that are at risk. With practical implementation and global acceptance, the principles that arise from this initiative may merit codification by Congress in the relatively near future.

Current State of Affairs and Trends

Since I last testified in February 2006 before the House Subcommittee on Africa, Global Human Rights, and International Operations and the Subcommittee on Asia and the Pacific and the Congressional Human Rights Caucus, the prevalence of Interne t censorship has continued to grow in scope and in depth. Our research through the ONI has identified over two-dozen states actively filtering Internet content, up from a handful five years ago. As access to information and communications technologies (ICTs) increases further, this trend seems likely to continue.

Technological innovations have fueled the expansion of Internet filtering and censorship, enhancing their sophistication and consequently creating troubling implications for human rights. Recent research suggests that several countries are investing in technologies that increase their capacity to target specific web pages, information sources, and applications. Surveillance technologies are likewise advancing, offering states expanded opportunities to eavesdrop on the communications of their citizens. Meanwhile, systems for storing and analyzing data continue to decline in cost, which allow governments to extract new information from data originally collected for other purposes.

A related and significant development is the growth of social media (including video and photo-sharing sites such as YouTube and Flickr, among others), which significantly amplify—and further complicate—unresolved tensions concerning content control. As these platforms are combined with other emerging technologies for content analysis, additional censorship and privacy concerns will also emerge.

Conflicts between differing privacy expectations, data retention laws and practices, and divergent approaches to traditional telecommunications and Internet communications regulation, give rise to increasingly hard problems. For example, Internet filtering and surveillance involves hardware providers, software providers, and service providers; US firms are not the only suppliers of these products and services. These factors remind us that issues of Internet freedom are part of a much larger policy and technology ecosystem, and accordingly, require care.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00124 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.085

The Corporate Dilemma

With over a billion people on the Net and about half the world having a mobile phone, more people than ever are using digital technologies and integrating them deeply into their lives and livelihoods. Governments are ever more cognizant of the double-edged sword that technology represents— as both a tool to foster economic growth and competitiveness, and as a potential threat to government sovereignty and power. As governments seek to control information and online activities, private actors, including ICT-related firms, are increasingly called upon to assist in carrying out those efforts.

In our recent book with our ONI partners, *Access Denied: The Practice and Policy of Global Internet Filtering*, we proposed a taxonomy that describes various types of companies and their involvement in these practices. We identified ICT firms as providers of hardware, software, online services, online publishing, telecommunications, and other content. Describing them in terms of function, we characterized their activities as **direct sales to governments of software and services** for filtering online content and for surveillance; **direct sales to governments of dual-use technology** for similar purposes; and **offering a service** that is subject to censorship, that censors publications, or requires personal information that could be subject to surveillance.[2] Considering these companies functionally is a useful way to examine their activities.

In past hearings, proposed legislation, and the public eye, perhaps the greatest focus has been placed on the activities of the most visible and widely known companies—those in the third category, offering online services. They face acute dilemmas, as they find themselves navigating between local law or practices that conflict with international human rights norms and US law, as well as their institutional values and those of their shareholders and users. Companies' considerations also include implications on their ability to do business and on their local employees. These companies, including Google, Microsoft, and Yahoo!, have shown sustained interest in resisting government demands to assist with censorship and surveillance, and a desire to engage proactively in developing strategies to address the human rights challenges they face. It is important to note that for each of these companies, a core business goal is to provide access to high-quality and secure information and communications services, and that their incentives are thus better aligned with the interests of their users than those of repressive governments.

Within this landscape, it is important not to neglect the companies selling software and hardware directly to governments, as they too form an important layer of the censorship and surveillance ecosystem, and have thus far been relatively silent on these issues. Moreover, there are a host of other US businesses that use the Internet to transmit data across borders —from banking and other financial services, technology licensing, news media, and hotel services— each of which may come into contact with government policies on free expression and privacy as they operate in different countries and across jurisdictions. In this testimony, we focus primarily on those who provide online services,

[2] Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT Press, 2008). See Chapter 5.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00125 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.086

because that is where we can lend the greatest insight, precisely because these companies have been willing to jointly explore the obstacles they face.

Conflicting law and dual purpose technologies
Mapping digital technologies onto the governance gaps created by globalization—and identified in the fine work of John Ruggie, our colleague at the Harvard Kennedy School and the UN Special Representative on Business and Human Rights—highlights multiple conflicting legal and normative regimes for companies to negotiate.[3] Governments may regard companies providing online services to their citizens as similar to their own national media and telecommunications companies—and therefore subject to the same expectations—regardless of the law of the company's home country or country of incorporation, its market orientation, or its physical presence in the country. They may expect these companies to adhere to laws and social norms about content parameters (ranging from intellectual property to pornography and national security), and to provide personal information about their users when requested for law enforcement purposes. Some governments have also shown a lack of understanding of how the Internet works—and what is realistically under the control of a company, and what, such as user-generated content, is not.

Companies likewise face a huge challenge as they seek to separate legitimate state requests from those that would require them to abridge human rights. For example, they must discern the difference between claims related to ongoing criminal cases, including kidnapping, terrorist threats, or child pornography, and those that seek to limit fundamental rights by stopping the flow of relevant public information or staunching peaceful political opposition. Thus, a priority must be the creation of effective internal systems (potentially with the support of US government conventions or systems), to enable thoughtful assessments of these types of requests, and to ensure that their responses are nuanced and appropriate, protective of the rights of specific citizens in addition to the rights to expression and privacy.

In addition to reaching a decision regarding the legitimacy of the request, companies must also consider the consequences of complying or not complying. Acquiescence to illegitimate requests may cause them to jeopardize their social and economic values by abridging core human rights. They may also incur risks such as losses in user confidence, brand identity, profit, and employee satisfaction, as well as the threat of legal (including shareholder) action. However, choosing to push back or initiate legal action can also generate risks. In choosing to resist law enforcement demands, companies may endanger operating licenses and institutional relationships, and more importantly, the potential safety of their employees on the ground. In the case of ill-chosen resistance, the risk can be broader, extending to public safety.

---

[3] John Gerard Ruggie, "Business and Human Rights: The Evolving International Agenda." *The Harvard Kennedy School*, Faculty Research Working Paper Series, June 2007.
Available at http://www.hks.harvard.edu/about/faculty-staff-directory/john-ruggie

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00126 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.087

Public Awareness, Pressure, and Understanding

Public awareness of these issues continues to grow. High profile violations of the rights to expression and privacy, shareholder actions, human rights campaigns, academic analysis, and Congressional interest have kept the pressure on. Companies are increasingly aware that the challenges they face are real and lasting and require a concerted and sustained effort in order to confront them effectively. The value of this rising awareness, however, will be greatest if accompanied by a deep understanding of the issues, so as to generate robust and dynamic solutions.

The cases that attract public attention are often extreme examples of the challenges ICT companies face. For example, China's censorship, manipulation, and detention practices are a real and immediate danger. However, associated media coverage does not span the range of issues nor reflect their complexity, but instead directs public attention to the elements that appear to be the most straightforward to understand. High profile cases are deeply unsettling at best, but they are closer to the sharp and menacing tip of the iceberg rising above the waterline than they are to the substantial and complicated dangers lying below it. The threat to digital expression and privacy is global and extends well beyond what is commonly reported, and the practices of any one state should not dominate our understanding and approach to solutions. We must address the complexities of the issues that lie beyond the public eye, bringing them to light with greater transparency and accurate data. Based upon that understanding, we will have a much stronger platform upon which to develop solutions that engage the wide range of stakeholders necessary to affect change.

Constructive Engagement

Despite the substantial human rights challenges that the ICT sector faces, the continued presence and constructive engagement of technology companies in these markets is critical. The tools, services, research, and even job opportunities offered by ICT companies bring social, economic, and political value through increased information and communication and through improved business and cross-cultural connections. They also hold great promise for international development. Furthermore, American businesses can positively influence the practice of government and local businesses, bring greater transparency to interactions that are often opaque, and provide a continued platform for informed government-to-government and government-to-company exchanges. A collaborative approach in which stakeholders create principles for operating in such regimes will, over time, generate opportunities for best practices development, improved processes, technological intervention, and creative and effective solutions.

Conversely, the disengagement of these stakeholders from foreign markets through overly prescriptive legislation would likely not improve the situation. Competitors to US companies are on the rise, and placing limitations on the engagement of US firms in these markets runs a very real risk of simply handing them to other companies who may be less open to constructive influence and may have a lower commitment to human rights. Thus, rather than focusing on limiting opportunities for US corporate activities, it is important

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00127 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.088

to address challenges to privacy and free expression so as to have a sustained influence on the behavior of companies based both in the US and around the world, as well as having a positive impact on the regulatory environment in which these companies operate overseas.

In an industry in which rapid change, innovation, and evolution dictate that these dilemmas will remain a moving target, and subject to shifting technologies, business models, regulations, and politics, the creation of an adaptive platform is essential. These challenges suggest the wisdom of establishing a collaborative approach for multiple stakeholders— including government, nonprofit, academics, and business— to come together for learning, coordinated action, increased transparency, innovation, and enhanced channels of communication, to promote a nuanced understanding of these issues. This process has been started and would benefit from broad support.

Recommendations on a Starting Point

Over the past two years, in partnership with the Center for Democracy and Technology and Business for Social Responsibility, in addition to other academic institutions, human rights groups, socially-responsible investors, and leading ICT firms, the Berkman Center has been involved in a collaborative initiative designed to identify solutions to the problems related to freedom of expression and privacy online.

As the Committee recognizes, these matters are complex. After two years of deliberation and study, we understand more clearly the nuances and complexities of the issues. We are still, however, far from defining solutions to these growing challenges. Furthermore, we believe that legislative action now that would prescribe what US companies can and can not do overseas would be premature and potentially damaging to the long-term objective of promoting greater freedom online.

This process represents a promising way forward, one that we believe will ultimately inform legislation and serve as a productive means of interaction with government. It calls on companies to develop a dynamic principles-based approach to ensuring that they operate ethically, consistently, and strategically (for human rights advancement) in these charged contexts, with an emphasis on strong internal rights-focused processes that are supported and informed by group collaboration, accountability, and transparency. While the Principles, Implementation Guidelines, and governance structure are not yet finalized, we expect that agreement and initiation of collaboration will take place in fall 2008, allowing us to focus exclusively on broadening, deepening, and improving our approach.

It is important that any legislation not be written so broadly as to attempt to confront every issue and actor with one set of rules, but neither should the law address one set of issues and ignore the others. A better approach is to promote the learning and integrated understanding that would lay the foundation for future legislation, ideally in conjunction with the Principles process.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00128 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.089

If the Principles that are currently being developed in the context of the multi-stakeholder process are implemented, grow in stability, and gain acceptance, they will be a good basis for future legislation to codify and bolster the norms that emerge.

We offer the following recommendations for your consideration, many of which have emerged from the Principles initiative:

1. Support Research, Learning and Awareness

Contribute knowledge and resources to improve understanding of online censorship, filtering, and surveillance practices. Facilitate the preparation of annual human rights reports that include assessments of the risks to freedom of expression and privacy with respect to ICT. Fund research into relevant legal regimes, events, and trends in Internet freedom, and make the results publicly accessible.

2. Create Alternative Paths

Fund and promote the development and dissemination of innovative technologies that promote Internet freedom. Contribute to education and awareness regarding online security.

Explore options for structured cooperation with foreign law enforcement by creating or adhering to a recognized, standardized, and streamlined process for legitimate requests for information from US companies, such that companies have guidance on the appropriate course of action, and pressure on companies to physically locate data in certain jurisdictions is mitigated.

3. Build Partnerships and Enhance Coordination

Create regular opportunities for open exchange between the ICT sector, human rights organizations, academic researchers, and the US government. Consistently and strategically raise concerns about surveillance and censorship in appropriate international bi- and multi-lateral fora.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00129 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.090

4. Create Incentives

The current multi-stakeholder initiative is a promising near-term approach to understanding and addressing the challenges faced by US companies providing services internationally via the Internet. The US government can best assist this effort by providing incentives to cooperate with this multi-stakeholder effort, and should avoid legal restrictions or penalties that could discourage cooperation.

Promote the compilation and sharing of information. Facilitate the sharing of information by companies on threats to free expression and privacy. Assist companies in tracking threats to free expression and privacy.

Recognize and reward legal, practical, organizational, and technical progress on these issues by countries, companies and other innovators.

5. Lead the Way

The US government can help to facilitate change in policy regimes worldwide by closely examining our own regime and then sharing resources with other countries willing to follow our lead.

Identify and address inconsistencies in US policy including privacy, data retention, surveillance, anonymity and speech, recognizing that a holistic US policy framework informs related approaches in other nations.

Assist countries in clarifying and improving their policy regimes with respect to ICT generally, and privacy and expression specifically.

6. Foster Transparency

In order to address fully the challenges in this sphere, we should encourage companies to be more transparent about the impact of their policies and practices on rights of privacy and freedom of expression. There are a number of ways that these companies can make their actions more transparent to users, more protective of civil liberties, and more accountable to all of us.

Encourage US companies to inform users about content restrictions or threats to privacy in a clear and timely manner, recognizing legal restrictions.

7. Codify the Principles

To extent that the multi-stakeholder Principles initiative leads to a workable solution, the US Congress should consider legislating this approach over time, much as Congress did with regard to the Sullivan Principles.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00130 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.091

Conclusion

The Internet has the capacity to foster active and participatory democracies around the world, and to advance and protect the human rights of expression and privacy. The rise of filtering, censorship, and surveillance practices worldwide has profound implications for the global development, proliferation and health of democratic values—such as privacy, access to information, participation, freedom of expression, and other human rights. Because the Internet is truly a global network that shows no sign of slowing down, the ramifications of restrictions within the online space should be of paramount concern to US policy-makers, and should inform their relationships and negotiations with governments worldwide. We support Congress' laudable effort to improve understanding of these important and timely issues.

There are significant challenges and complex ethical dilemmas across this landscape for corporations, governments, and users. At this relatively early stage of our understanding, any legislative approach should support adaptive, realistic, and engagement-oriented efforts by companies operating in these contexts. We must buttress any legislative approach with increased knowledge, communication, study, and coordination to help turn back threats to human rights. Ultimately, while the measures we and others have offered will hopefully increase Internet freedom, the only truly reliable way to reduce excessive filtering and inappropriate surveillance is via a change of policy within the countries where this occurs.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00131 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.092

Reporters Without Borders USA
1500 K Street, NW, Suite 600
Washington DC 20005
Tel: 202 256-5813
Email: lucie.morillon@rsf.org

Senate Subcommittee on Human Rights and the Law
Committee on the Judiciary

Statement on record

Lucie Morillon,
Washington Director,
and
Clothilde Le Coz,
Internet Freedom Director,
Reporters Without Borders

Hearing on "Global Internet Freedom: Corporate Responsibility and the Rule of Law"

May 20, 2008

Reporters Without Borders would like to thank Chairman Durbin for giving us the opportunity to present this statement on record today, and for taking the leadership on this issue in the Senate.

In this rapidly expansive information age, the new media, including the Internet, has been creating plenty of opportunities for those seeking to enjoy the free flow of information online. Citizen journalists and bloggers have known how to use the power of the Internet. Recently, in Egypt, some officials were sent to jail after reports of torture in Egyptian prisons were posted online. But these opportunities are being offset by increasing repression by authoritarian governments who won't tolerate any expression of dissent. They are ready to do whatever it takes to control the Internet,by filtering it, banning key words, intimidating users—and they are enlisting the help of Western companies to do so. The battle of information is no longer being played out only within the mainstream media. It has taken over the Internet.

As of early 2008, Chinese Internet users became the most numerous web surfers in the world. This

45688.093

situation raises the legitimate issue of the appeal that this huge market they represent will ultimately have (210 million people). Since the start of the 21st century, American Internet sector companies have agreed to sign contracts with the Chinese authorities without the issue of human rights ever being a significant consideration in these negotiations.

In 2005, the Shi Tao case showed the consequences of collaborations between repressive regimes and Internet sector companies. Yahoo! had to concede its share of responsibility in the arrest of this journalist, who, by disseminating information via the Internet, was accused of "subverting the power of the State." He received a ten-year prison sentence. Yahoo! made it possible for the authorities to identify Shi Tao by disclosing his personal data. The media picked up the story, and Yahoo!'s brand image has been seriously damaged ever since.

Nevertheless, some American companies present in China are still supplying material that allows government authorities to censor the content of certain Internet websites and monitor the Web. Others are adopting rules inconsistent with the freedom of expression that they all claim to uphold as one of their corporate values.

I - A GLOBAL PROBLEM?

Reporters Without Borders is an international press freedom organization. For more than twenty years, we have been striving to defend and promote the right to inform and to be informed around the globe. Because of the success of the Internet, we are seeing freedom of expression violations on the Web every day. Currently, 65 cyberdissidents—most of whom are in China—are behind bars for having exercised their right to be informed and to express their opinions on the Web.

Five years ago, most Internet censorship seemed to be taking place in China and Saudi Arabia. Since then, the trend has spread to other countries. China is not the only country that restricts the circulation of information on the Internet; some 30-odd countries are now practicing some form of this censorship. Reporters Without Borders has designated 15 countries as "enemies of the Internet." They are: Belarus, Burma, China, Cuba, Egypt, Ethiopia, Iran, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, Vietnam, and Zimbabwe.

The organization also singled out 11 "countries under watch." They are: Bahrain, Eritrea, Gambia, Jordan, Libya, Malaysia, Sri Lanka, Tajikistan, Thailand, United Arab Emirates and Yemen. Unlike the "enemies," these countries do not massively imprison bloggers or censor the Internet. But they are apparently sorely tempted to do so, as abuses are common. Many of them have laws that they could use to gag the Internet if they wish, and judicial or political authorities often use anti-terrorism laws to identify and monitor government opponents and activists who express themselves online.

Cases of proven collaboration between Western companies and Internet censors are so far limited to a few countries (see below), but they may well spread if nothing is done. The next Shi Tao case may very well be Vietnamese or Syrian.

45688.094

II – EXAMPLES OF COLLABORATION BETWEEN AMERICAN COMPANIES AND REPRESSIVE GOVERNMENTS

CHINA

Google is cultivating an ambiguous position in matters of censorship

Google allows users to remain anonymous by concealing their IP addresses, at their request. However, since 2006, the company has agreed to censor the Chinese version of its search engine (google.cn). Google.com is still accessible, but certain content is filtered by the authorities. For example, during the Lhassa demonstrations in March 2008, no headline about Tibet appeared in Google.com's "News" menu.

However, search engine censorship is a basic freedom of expression issue. According to the most recent study by the China Internet Network Information Center (CNNIC)—an official Chinese agency—72.4% of the information is obtained on the Chinese Network using this type of tool.

It is true that the company has shown more transparency by informing google.cn users that their research results are being screened. However, this disclaimer notice appears regardless of what research is being done. The user therefore does not know what content is really blocked.

What is more, Google is co-financing Baidu, the Chinese search engine that has cornered 60% of the market. The country's most popular search engine is also the one most censored.

Baidu scrupulously filters "subversive" content. When Google was blocked, in 2002, Chinese websurfers were unsurprisingly redirected—to baidu.com. Moreover, Chinese authorities are expecting baidu.com to replace every "erroneous" (or censored) page an Internet user may happen to stumble upon.

The geographic search engine, "GoogleEarth," has also been targeted. Authorities have censored certain parts of the maps it displays and redesigned borders on the pretext that they pose "a threat to national security." This measure concerns some 10,000 Chinese mapping websites.

Can we still trust Yahoo!?

The "Shi Tao" case highlighted the role that corporations are playing in Chinese censorship. In 2004, Yahoo! provided the journalist's IP address to the authorities, which enabled them to arrest him. He was sentenced to 10 years in prison for "illegally divulging state secrets abroad." In 2007, the company's CEO apologized to the cyberdissidents' families before the U.S. Congress, and created a humanitarian fund on behalf of such families, which unfortunately leads us to believe that Shi Tao is not the only one.

Yahoo!'s collaboration was also established in three other cases:

45688.095

1) Li Zhi, a former civil servant, was sentenced in 2003 to eight years in prison. The verdict mentions that the American company Yahoo!, as well as a local competitor, Sina, collaborated with Chinese court officials. It indicates that Yahoo! Hong Kong Ltd and Sina Beijing provided information that enabled the officials to confirm that Li Zhi had created an e-mail account on their websites. It does not, however, indicate whether the content of the messages sent or received by the cyberdissident was also transmitted to court authorities.

2) On November 18, 2003, Jiang Lijun was sentenced to four years in prison for "inciting subversion." He stands accused of having tried to impose democracy by "violent means." The police considered the cyberdissident to be the leader of a small group of cyberdissidents. According to the verdict, Yahoo! Holdings (Hong Kong) has confirmed that the e-mail account ZYMZd2002 had been jointly used by Jiang Lijun and another pro-democracy activist, Li Yibing. In a paragraph headed "physical and written evidence," the document also stipulates that a "declaration" dated September 25, 2002 had been found in the e-mail "Drafts" folder associated with this e-mail box, without specifying whether this information had been provided by the California-based company. The access codes could also have been provided by Li Yibing, who is suspected of having been a police informant in this case.

3) Wang Xiaoning was sentenced in September 2003 to 10 years in prison for posting "subversive" articles that were distributed over the Internet. The verdict also refers to Yahoo!'s collaboration. This document states that information provided by Yahoo!'s Hong Kong branch helped to establish a link between Wang Xiaoning and messages carried by a discussion forum. It specifies that the moderators of this discussion group hosted by Yahoo! had decided to ban the cyberdissident from using the forum.

In 2007, during a hearing before the U.S. Congress House Committee on International Relations, Yahoo!'s CEO, Jerry Yang, publicly apologized to Shi Tao's mother, who was present, and decided to set up a humanitarian fund be set up to assist the families of cyberdissidents imprisoned in China.

The company also censors its search engine's results. In 2002, it agreed to sign a "Public Pledge on Self-Discipline for the China Internet Industry," pledging to comply with the censorship constraints imposed by the Communist Party.

In the spring of 2008, Yahoo! wrote to Condoleezza Rice to ask that she intervene with her Chinese counterparts in order to secure Shi Tao's release. This move is one of a few recent encouraging signs that contrast sharply with the attitude of a company which, in 2005, refused to apologize for its actions. Nonetheless, if this admission of responsibility and the measures taken to mitigate the situation represent a positive change in the position of Yahoo!'s leadership, its mode of operation in China does not seem to have changed. From this point on, another Shi Tao case can surface at any time.

During the recent demonstrations of March 2008 in Lhassa, Yahoo! asked for an informant to step forward by directly calling upon Internet users to denounce the Tibetan demonstrators on the "homepage" of their Chinese website. Twelve pictures of Tibetan agitators were posted and

45688.096

Internet users were encouraged to call a phone number connected to a Chinese police department. Within scarcely three hours, one rioter had already been identified and arrested. Another gave himself up.

Can we still trust a company that is willing to collaborate in this way with Chinese authorities and who is helping to worsen the status of human rights in the country by facilitating the arrest of individuals opposed to the regime?

Despite a few noteworthy efforts, Microsoft may be helping to eradicate anonymity on the Web

In 2005, the company agreed to censure its blog tools, Live Spaces, and became the second American company to agree to collaborate with Chinese authorities (after Yahoo!). Words such as "freedom," "democracy," or "Dalai Lama," are filtered and do not appear on these blogs.

After the negative publicity that targeted Microsoft when it announced that it was closing down Michael Anti's blog, the firm announced two series of measures in 2005:

- It will remove access to blog content only when it receives a legally binding notice from the authorities stating that this content is in violation of local law;
- This content will be removed only in the country in which it violates local law. The blog content will still be accessible to the rest of the world.

In 2008, the company announced that it planned to set up one of its biggest research laboratories in Beijing, which only fuels our fears about the research being done in China. One year earlier, the May 16, 2007 issue of the American magazine *The New Scientist* reported that one of the company's Chinese laboratories is working on a software program designed to analyze Internet user behavior (based on age, sex, etc.) in order to develop "intuitive" software that will pinpoint the type of Internet user visiting these websites, all for purely marketing and ad-targeting purposes. However, American companies who are claiming their right to carry out this type of procedure simply because they must comply with "local laws," could be induced to put the websites websurfers visit on file, again by order of the Chinese authorities, but without finding that disconcerting. In fact, Chinese authorities are striving to eliminate anonymity on the Internet, and this type of research is helping them to do just that.

On May 22, 2007, the Internet Society of China (ISC) asked several local and international companies to sign a "self-discipline code" to encourage cybernauts to identify themselves, and which all local search engines have applied—including Microsoft and Yahoo.cn, even though they stated that they would refuse to apply the clause requiring Internet users to register their online visits.

Cisco contributed to the root of Chinese censorship

45688.097

This company has sold routers (a software or hardware tool for directing data through a network linking several servers) to the Chinese government that censor certain Internet website addresses. Despite this technological involvement, which can adversely affect the company's image, the shareholders refused to vote for a resolution in 2006 which asked that a report be published within six months, at nominal cost, establishing a list and an evaluation of the practical measures that the company might reasonably take to reduce the probability that its business practices could lead to more human rights violations—particularly those involving freedom of expression, and cause more fragmentation of the Network.

Several months prior to Cisco System's General Meeting, at a hearing before the House of Representatives' Committee on International Relations, Mark Chandler, Cisco System's Senior Vice President and General Counsel had stated: "*Cisco sells its products, including Internet and surveillance technology, primarily through resellers, to government agencies and state-owned entities throughout the world. The U.S. State Department and others have documented how various governments, including several governments with which our Company does business, monitor, censor and jail Internet users, through manipulation of Internet technology.*"

Cisco Systems explains that it is not responsible for the way some products are being used. However, the company helped to build the Chinese Internet and some people are wondering what role Cisco's technicians may have played in setting up the Chinese Web's surveillance arsenal. An equipment contract of that magnitude rarely comes along without a comprehensive technical assistance contract.

IRAN

Paradoxically, the embargo that the United States has chosen to enforce against this country in view of the Iranian refusal to suspend its sensitive nuclear activities, is involving Americans in the Iranian censorship game. More and more American companies are withdrawing from the market because of the economic sanctions adopted by the UN in October 2007. For example, Iranian websites are more infrequently hosted by foreign servers, so they are now easier to censor. Likewise, cybernauts have access to Webmails less and less often (even though they are harder to monitor), because Iran is categorized as a "dangerous country," with which no one should deal.

In November 2007, **Yahoo! and Microsoft** removed Iran from their list of Webmail services, which are more difficult to monitor than traditional mail accounts controlled by a local server. Gmail (Google) is still accessible.

Godaddy, a web hosting and Internet domain name registrar, has had its participation in the Iranian market on hold since 2005 as a result of these sanctions. By deciding to no longer host Iranian websites, American companies are forcing them to rely on Iranian hosting companies, which are much more strict about censoring content.

Most of the opposition Internet websites are hosted by foreign companies because they cannot be legally banned, since their servers are based abroad. They can only be filtered.

45688.098

Furthermore, the filtering technologies are supplied by **Secure Computing** (San José, California), via "SmartFilter" software that allows users to block Internet website addresses. According to Secure Computing, this software makes it possible to block millions of websites in over 60 categories. It is therefore easy for the Iranian government to block websites for political reasons. "SmartFilter" is programmed to block websites hosted abroad as well as locally. (Beware: according to Secure Computing, the company has never sold an ownership license to Iran, so the government may be using it illegally!)

VoIP.ms (an Internet-based cell phone service) does not register the IP addresses of Iranian users because of the economic and financial sanctions imposed by the UN.

The company **Websense, Inc.** (San Diego) supplies filters used by the main Iranian ISP, ParsOnline.

YEMEN

According to the Open Net Initiative team's tests, Websense software (San Diego) is used by Yemeni authorities. The extent of the company's involvement is unknown. Is Yemen using its product legally or not? Yemen's main ISP, TeleYemen, blocks websites corresponding to the categories "content reserved for adults," "gay, lesbian or bisexual," "sexual education," as well as the majority of contents classified as "adult." But TeleYemen also has a category called "user-defined," that allows other sites to be blocked on the basis of other criteria.

Yemen is an example of those countries who could restrict the Internet in the near future and where the use of US products have been taken out of the hands -- and control -- of the American companies.

It has been said the presence of Western IT companies in authoritarian countries can help open up their societies. It is true, as far as these companies set higher standards in terms of freedom of expression than their local competitors. This is not a case of business as usual.

III - CONSEQUENCES OF THESE ETHICAL FAILURES

We believe that these practices violate international law and the right to freedom of expression as defined in Article 19 of the Universal Declaration of Human Rights, which was proclaimed by the United Nations when it was founded and is meant to apply to everyone—business corporations included.

Such ethical failings on the part of American companies damage the image of the United States abroad. Access to Voice of America and Radio Free Asia's websites, whose funding comes from the IBB, has been regularly blocked on the Chinese version of Yahoo! and Google. These

45688.099

companies owe U.S. taxpayers an explanation for why and how their money is being used to pay for the consequences of these firms' collaboration with China's censors.

Internet companies were created to facilitate information access for all. Yet some companies now find themselves in the awkward position of collaborating with Web censors in an effort to alter the very nature of the product they are selling. By collaborating with repressive regimes' censorship policies, they are helping to create country-specific access to multiple versions of the Internet. They are putting borders on this universal arena of communication that the Internet was intended to be.

The Internet is used in China to channel and influence public opinion, especially in support of nationalistic sentiments, against China's enemies, and to promote Communist Party propaganda

Internet censorship in China subverts U.S. diplomacy efforts to promote democracy in the world. By helping Chinese authorities to crack down on dissidents and control the free flow of information online, some U.S. IT companies are indirectly helping to block political changes in the country, thereby preventing China from following the path to democracy.

Business decisions made about markets based in Internet-restrictive countries cannot brush aside the issue of human rights if we want to prevent U.S. companies from being turned into a tool for repression. How can American companies still do business in China without compromising international standards for human rights or the viability of their operations? There are no miracle solutions, but the recommendations listed below should help them stand their ground on the issue of user privacy and basic human rights. We believe the fear of being thrown out of the Chinese market is overstated. The Chinese authorities still need the know-how of these major IT firms and there are reasons to believe that they would not dare take measures that would be seen as business-hostile, and thereby compromise investors' trust.

IV - RECOMMENDATIONS

At the technical level:

- An appropriate filtering policy

Any Web-filtering measure is typically introduced because of a security concern (parental filter, for example). This is one of the reasons why it is easy to find them on the market. Couldn't the companies that sell these software programs to repressive countries design them in such a way that certain words such as "democracy," or "human rights" could not be filtered, thus guaranteeing that their users can access at least a minimum amount of information?

- Development and better publicity of user empowerment tools to get around censorship.

Companies could help already-existing software whose developers lack the necessary funding (Psiphon, TOR) to become more accessible (by advertising them, providing links on their

45688.100

homepages, or just by financing research for these projects). Creating a fund to promote research on ways to bypass Internet censorship would allow this problem to be addressed and demonstrate the companies' good faith and their desire to ensure that information can truly continue to circulate freely on the Net.

At the policy level:

These companies need to adopt a self-regulation policy and incorporate provisions in their methods of operation which will guarantee the respect of international human rights standards. Some of the provisions that should be taken into account are:

- a ban on having local servers in repressive countries;
- agree not to store personal data that would allow Internet users to be identified on the very territory of countries that refuse to respect freedom of expression on the Internet;
- agree not to be "proactive" in matters concerning censorship;
- legally challenge the requests of authoritarian regimes (ask for written legal binding requests).

The adoption of a voluntary set of principles by ICT companies would bring us a lot closer to realizing these goals than a multitude of individual initiatives.

Discussions between some of the companies, academics, NGOs and stakeholders have been going on for about 2 years, facilitated by nonprofit business associations Business for Social Responsibility (BSR) and Center for Democracy and Technology (CDT). The success of these discussions is as yet uncertain. The companies should not only agree on how to legally challenge government requests that could potentially violate human rights and users' privacy, but also allow an independent monitoring procedure to assess the latter's compliance with these principles. Cisco Systems is not part of this process.

Any voluntary set of principles, however, would not prevent another Shi Tao case from happening, for even if the companies can challenge the requests—by asking for written requests instead of just a phone call, for example—they are still facing governments that require them to abide by local laws. Some companies complain that this is a government-to-government issue. They need a shield that will protect them from being directly answerable to governments. The Global Online Freedom Act (GOFA) introduced by Representative Chris Smith (R-NJ) would do exactly that: put the U.S. government directly between U.S. companies and the Chinese government. Requests about these companies' users' information would have to go through a process vetted by the U.S. Justice Department and inquirers would have to prove that this is a legitimate law enforcement issue. The number of requests coming from authoritarian governments would then very likely drop, and they would have to find another way to go after dissidents—*without* the complicity of U.S. firms.

Other interesting provisions of the bill would require the U.S. companies concerned not to locate the servers containing personal identifying data in territories controlled by such governments, putting them out of these countries' jurisdiction. The companies would also have to act transparently and transmit information about the type of censorship they apply to an interagency-

45688.101

staffed Office of Global Internet Freedom, whose job it would be to define U.S. government policy for the promotion of the free flow of information online and to monitor violations. The bill also calls for the drafting of a voluntary code of conduct. Companies that do not comply with the GOFA's provisions—especially with regard to the protection of user data —would be sanctioned. The GOFA would also provide for a feasibility study to control the exporting of equipment, software and applications sold by U.S. Internet sector companies to countries the White House designates as repressive.

Senate legislation addressing the same issues as the GOFA—especially the issue of personal identity data protection—is crucial to preventing American companies from being forced to collaborate with repressive regimes in their dissidents' witch hunt.

Reporters Without Borders is ready to offer its assistance to you and to this subcommittee on this important issue.

45688.102

Opening Statement of Michael Samway
Vice President & Deputy General Counsel for Yahoo! Inc.
Hearing Before Senate Judiciary Committee
Subcommittee on Human Rights and the Law
May 20, 2008

Chairman Durbin, Ranking Member Coburn, Members of the Subcommittee, my name is Michael Samway and I am Vice President and Deputy General Counsel at Yahoo! Inc. I also lead Yahoo!'s global human rights efforts. I appreciate the opportunity to testify before you today.

At Yahoo!, we are deeply committed to human rights and to being a leader among technology companies in this area. Our company was founded on the principle that promoting access to information can fundamentally improve people's lives and enhance their relationship with the world around them. In the period since Yahoo!'s creation in 1994, the power and ubiquity of the Internet has exceeded even our most far-reaching expectations.

The Internet has dramatically changed the way people obtain information, communicate with each other, engage in civic discourse, conduct business and more. Even in countries that restrict people's ability to communicate with one another or access information, people are still finding meaningful ways to engage online. Over the last week alone, we have seen just how important new communications technologies can be in places like China. Internet and cell phone resources have proven invaluable as government authorities and individuals contend with the aftermath of a devastating and enormously tragic earthquake in Sichuan province.

With the goal of bringing Yahoo!'s technological tools to people around the world, we embarked on a mission to expand our business globally in the late 1990s. As one of the first Internet companies to explore the Chinese market, we launched a service with the belief that providing the people of China with innovative tools to communicate, learn, and even publish their own views was one effective means to improve their way of life.

We were joined in this strategy of engagement by many in the United States Congress and in both Democratic and Republican administrations alike. With the sporadic pace of political

45688.103

progress in China as well as the need for companies there to adhere to local laws, we've also learned that expanding into emerging markets presents complex challenges that sometimes test even the important benefits of engagement itself.

While Yahoo! has not owned or had day-to-day control over Yahoo! China since 2005, we continue to be concerned about the challenges we faced in that market and will certainly face in other markets in the years to come.

Skeptics have questioned whether American Internet companies should engage in these countries at all. Yahoo! shares these concerns, and we have confronted these same questions about engagement in challenging markets. Yet, we continue to believe in the Internet's transformative power and, on balance, its constructive role in transmitting information to, from, and within these countries. And we are committed to doing our part through supporting individual and collective action.

Governments – because of their enormous leverage – have a vital role to play. To that end, we have asked the U.S. government to use its leverage – through trade relationships, bilateral and multilateral forums, and other diplomatic means – to create a global environment where Internet freedom is a priority and where people are no longer imprisoned for expressing their views online.

Our CEO Jerry Yang has met personally with senior State Department officials, and earlier this year wrote a letter to Secretary Rice urging the State Department to redouble its efforts to secure the release of imprisoned Chinese dissidents. Secretary Rice subsequently raised this issue with senior Chinese officials, and since then we have seen Members of Congress echo this call for U.S. diplomatic leadership. We hope these efforts will both intensify and bear fruit.

We are also taking steps on our own. Jerry Yang announced the Yahoo! Human Rights Fund in November 2007, as part of a broader effort to address human rights challenges in China and around the world. We have partnered with noted dissident and human rights activist Harry Wu, who is here with us today, and the Laogai Research Foundation to establish this fund. The

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00143 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.104

Yahoo! Human Rights Fund will provide humanitarian and legal support to political dissidents who have been imprisoned for expressing their views online, as well as assistance for their families. A portion of the fund will also be used to support the Laogai Research Foundation's educational work to advance human rights.

In order to fuse our global business with responsible decision-making on human rights issues, we have also established the Yahoo! Business & Human Rights Program. A key pillar of this program is a formal assessment of the potential human rights impact of business plans we develop for new foreign markets. This assessment examines the human rights landscape in a country, evaluates potential challenges to free expression and privacy, and offers strategic approaches to protect the rights of our users through legal and operational structures, among other methods. Yahoo! then tailors its entry into the new market to minimize risks to human rights.

Because it is so difficult for just one company to create systemic change, Yahoo! has also been a committed participant in a broad-based global human rights dialogue. We are working with industry partners, academics, human rights groups, and socially responsible investors to develop a global code of conduct that will guide technology companies operating in challenging markets. At Yahoo!, we are eager to make this global code a reality in the near future.

As an industry pioneer, Yahoo! is proud to have explored new ideas and markets, helping drive the transformative power of the Internet. Just like others who have gone first, Yahoo! has also learned tough lessons about the challenges of doing business in nations with governments unlike our own. Yahoo! is working intensively and at the most senior levels in the company to set the highest standards for decision-making around human rights. The initiatives we pursue at Yahoo! are intended to protect the rights of our users, improve their lives, and make the extraordinary tools of the Internet safely and openly available to people around the world.

I appreciate the opportunity to tell you about these efforts to date and about our plans to continue pursuing a global leadership role in the field of human rights. I look forward to answering your questions. Thank you.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00144 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.105

Testimony of Nicole Wong, Deputy General Counsel, Google Inc.
U.S. Senate Judiciary Committee Subcommittee on Human Rights and the Law
Hearing on "Global Internet Freedom: Corporate Responsibility and the Rule of Law"
May 20, 2008

Chairman Durbin, Ranking Member Coburn, members of the subcommittee.

Thank you for inviting me to discuss with you the issue of internet freedom and Google's efforts to maximize online freedom of expression and access to information. My name is Nicole Wong, and I'm Google's Deputy General Counsel. In that role, I am responsible for helping to address limits on free speech that Google faces around the world.

Google's commitment to freedom of expression is at the core of everything we do. Our company's mission is to organize the world's information and make it universally accessible and useful. We provide internet users with products like our search engine, Google Maps, and YouTube that let them quickly and easily share, receive, and organize digital information. In theory, any person – regardless of who she is or where she lives – can use these free products that enable free expression and information sharing.

The internet continues to be a powerful medium for propagating political opinions, religious views, and other core speech. And that trend has been accelerating. The estimated number of blogs has grown from fewer than two million in 2004 to more than 110 million this year. Expression through online video has become so popular that ten hours of videos are uploaded to YouTube every minute, and hundreds of millions of videos are watched on the site everyday. Even in countries where governments engage in heavy censorship, the internet has nevertheless proven to be an effective tool for sharing information and promoting political change.

However, the freedom of expression that's generated by blogs, social networks, video sharing sites, and other speech tools available on the internet is not embraced universally. As a global internet company operating in more than 150 countries – all with different national laws and cultural norms – we face daily challenges to our goal of making sure that the internet is a global platform for free expression.

With that in mind, I would like to make four main points in my testimony this morning:
First, our products are above all else platforms for free expression and access to information.

Second, a wide range of legal and cultural barriers around the world regarding the free flow of information impact our products and services every day.

Third, we are working hard to respond to these challenges through policies and technology that promote free expression.

45688.106

And finally, we believe that governments around the world can and must do more to effectively reduce internet censorship and promote free expression online.

Google's products are open platforms for free expression

Most of our products – offerings like Blogger (our blogging service), Groups (our online bulletin board), orkut (our social networking site), Google Apps (our suite of collaborative productivity tools), and YouTube (our video sharing service) – are open platforms for free expression for which we do not generate the content. We do not serve as a gatekeeper and Google employees generally do not check content before it goes live, just as your phone company would not screen the content of your phone calls or your Internet Service Provider (ISP) would not edit your emails before you hit the "send" button.

Our products are often used as free expression tools in countries that restrict speech through other media. For example, in May 2007 Venezuelan President Hugo Chavez refused to renew the broadcast license of Venezuela's Radio Caracas Television on the grounds that RCTV violated broadcast laws, supported a failed coup against him in 2002, and more generally offered an anti-governmental perspective.

Despite protests by thousands in the streets of Caracas, the Venezuelan government replaced RCTV on May 28, 2007 with a state-run broadcast station. On that same day, RCTV's news department created a channel on YouTube on which it began airing daily installments of its newscast *El Observador*. Since then *El Observador* has been viewed more than 850,000 times, and many of RCTV's videos on YouTube have generated lively debates about freedom of expression. The inaugural post in response to the first *El Observador* video exclaims, "¡Viva la libertad de expresión!" (in English, "Long live freedom of expression!")

In other countries we have seen that communication platforms like internet video sites and blogs may be the only means for speech to emerge from communities closed off by authoritarian governments.

For example, when the military government of Myanmar (Burma) cracked down on protests by tens of thousands of Buddhist monks in the fall of 2007, it tried to do so outside of the public eye. During the protests, foreign journalists were kicked out, national media was shut down, and internet and cell phone service was disrupted within Myanmar in an effort to prevent information leaking out about the extent of the violence.

Nevertheless, tools like Blogger and YouTube were used by citizen journalists to share videos of the protests and information about the extent of the blackout, enabling the rest of the world to understand the human rights abuses taking place within the country.

As our Venezuela and Myanmar experiences indicate, our products are platforms for free expression, transparency, and accountability. Because of this, we often face efforts by governments throughout the world to restrict or deny access to our products.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00146 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.107

Censorship challenges that Google faces

Most governments around the world have formal provisions for the protection of freedom of expression in their constitutions or fundamental laws. Indeed, the Universal Declaration of Human Rights, adopted by the United Nations General Assembly in 1948, includes language that almost seems to have been written in anticipation of the borderless internet:

> *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.* [UDHR, Article 19]

Despite such formal undertakings, it is clear that many governments impose legal or practical limits on their citizens' freedom of speech. These limits on free expression take many forms. Some limitations are laudable and reflect shared moral imperatives such as the fight against child pornography. Others are rooted in culture and history, such as Thailand's laws against insult to the King, Germany's laws against Nazi propaganda, and India's laws against insulting religion or religious beliefs. And finally, of course, some governments, such as China, Iran, North Korea, Zimbabwe, and Myanmar, have imposed varying levels of political censorship.

Over the past several years, Google has encountered a wide array of governmental limitations to free expression online. Because our technologies and services enable every person with an internet connection to speak to a worldwide audience and, conversely, to read the words and watch the images posted beyond her nation's borders, Google has become a regular focus of governmental efforts to limit individual expression.

In my testimony today, I'd like to give you a sense of the scale and nature of these governmental efforts, and to explain how Google has attempted to promote freedom of speech while navigating the different governmental demands to limit access to information.

- ***YouTube***: Since 2007, our YouTube video sharing site has been blocked in at least 11 countries including China, Thailand, Turkey, Pakistan, Morocco, Brazil, Syria, Indonesia, Iran, Saudi Arabia, and Myanmar.

- ***Blogger and Blog*Spot***: In the last couple of years, we have received reports of our Blogger and Blog*Spot blogging sites 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.

Though we do not believe that it is ever justifiable for a country to block one of our services in its entirety, it is notable that the stated rationales for these instances of blocking range from relatively benign, apolitical, and culturally- and historically-driven content regulations all the way to heavy-handed political censorship directly contrary to basic international standards of political, religious, academic, and cultural freedom of expression.

To fill out this picture, here are three examples of government efforts to restrict expression that resulted in the outright blocking of YouTube for a period of time:

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00147 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.108

- ***Turkey and the Ataturk videos.*** YouTube has been blocked in Turkey repeatedly over the past year because of videos deemed insulting to Mustafa Kemal Ataturk, the founding father of modern Turkey, and other videos deemed by the Turkish government to be threatening to the state, such as videos promoting an independent Kurdistan. Under Article 301 of Turkish law, it is a crime to denigrate Turkishness, to threaten the unity of the Turkish state, or to defame Ataturk. As a result, Turkish courts have ordered the entire YouTube site blocked multiple times, and for several days, because of videos deemed illegal in Turkey. While we have been engaged with Turkish officials for many months, it has been very difficult to even know what videos have been the source of complaint.

- ***Indonesia and the "Fitna" film.*** Earlier this year, the controversial short film "Fitna" was uploaded to YouTube. Produced by a Danish politician, the film mixes clips of terrorist acts and propaganda and passages from the Koran to critique Islam in a manner offensive to some viewers. In Indonesia, high-level government officials publicly demanded that YouTube and other sites hosting the video immediately remove the content, in order to minimize the odds of violent protest riots. The government ordered Indonesian ISPs to block the entire YouTube site, preventing users within the country from viewing any videos. This had the ironic effect of blocking dozens and dozens of videos criticizing and responding to "Fitna" from Indonesians. We engaged in a dialog with the Indonesian government to determine what videos they objected to, and worked with local counsel to assess whether the videos violate Indonesian laws against hate speech. In the face of public pressure over the censorship and without further guidance from the government, Indonesian ISPs began lifting the site-wide block. It is our policy to only narrowly remove illegal content for the jurisdiction in which it is banned. As such, Google subsequently took steps to block the "Fitna" video from being viewed within Indonesia due to its likely illegality, but kept it available to users in all other countries.

- ***China and YouTube.*** In October 2007, at a time when the Dalai Lama was awarded the Congressional Gold Medal and the Communist Party Congress convened in Beijing, YouTube was blocked throughout China. While we were not informed of the exact cause of this suppression of speech and we did not ourselves remove any videos from YouTube, access to the site in China was reinstated following the conclusion of the Party Congress.

As these examples indicate, despite our efforts to minimize restrictions on speech, we routinely face situations where governments attempt to limit expression through our products.

A broad range of global censorship efforts

As noted above, some censorship efforts are relatively benign and stem from factors such as cultural sensitivities and history. For example, when reported to us, we remove links to content that promotes violence against protected groups from the search results for our Canadian search engine, Google.ca, because such content is illegal under Canada's Human Rights Law.

On the other end of the spectrum are governments that prohibit commentary or criticism on certain political or otherwise sensitive topics.

Some of these efforts affect our global products; others affect a localized version of our products we

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00148 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.109

have created to better serve a country market. For example, we have launched our search service in Spanish for Argentina. That service is located at www.google.com.ar, and because it is associated with Argentina's top level domain (".ar") and has various other links to Argentina, we apply Argentine law to our removal decisions. By contrast, we do not apply non-US law to the removals from our search service located at www.google.com.

Generally speaking, this distinction allows us to provide .com services with few restrictions on content and localized services with restrictions relevant to the local jurisdiction. The Google.ca example above is illustrative of this point. Another example is what we do in Germany, which bans the promotion of Nazism. German law makes Nazi content illegal, so we remove such content from our products hosted on our German domain, Google.de, when we become aware of such material. However, we do not remove Nazi content because of German law from our global products hosted on Google.com.

On a practical level, these different laws result in a variety of national standards on what can be restricted, which often poses difficult challenges for our services that can be accessed by a global audience. And these legal differences pose not only compliance difficulties but also real technical challenges. Restricting content that is perfectly legal in one country but illegal in another is not easily done on global internet services.

National governments often lack the technical ability and tools needed to address illegal content in a granular fashion, which often results in blocking access to a product as a whole, rather than just to a particular video or blog post. For example, earlier this year, Pakistani concern over an anti-Islamic video actually resulted in a global outage of YouTube after a national ISP erred in implementing orders by that government to block YouTube within the country. Global users of YouTube, including those in the U.S., were redirected to a non-existent site, and they were therefore unable to access the service for several hours.

The case of China

China is a case that has posed for us all of the legal and technical hurdles described above, along with other challenges.

For several years prior to 2006, Google experienced widespread blocking of or other interference with our global search service, Google.com in China. To respond to this interference, in 2006 we launched Google.cn, a filtered search service that operates in China in conformity with local laws, regulations, and policies on illegal content. In doing so, and to provide transparency to our users in China, we became the first search engine in that country to post a notice on the search results page when certain links have been removed. Google.cn has not been subject to outright blockage.

Our Google.cn website supplements, and does not replace, our unfiltered (but periodically interrupted) Chinese-language interface on Google.com. Google.com remains open for Chinese-speaking users worldwide, including within China, when it is not being blocked by the government.

Let me stress that the decision to operate a filtered search engine at Google.cn was a difficult one. It was reached after more than a year of analysis and discussion by our senior management, and we continue to debate how to best operate in China.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00149 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.110

The decision was based on a judgment that Google.cn would make a meaningful – though imperfect – contribution to the overall expansion of access to information in China. To date, we believe that on balance the decision to operate in China was the right one because our presence in China has led to improvements in freedom of expression.

For example, we believe that more internet users in China can access more information outside of China through Google.cn than through other offerings. In addition, our engagement in China through Google.cn has driven industry advances in transparency to users. Today, leading search engines in China, including the market leader Baidu, have followed our lead and now provide disclosures when they remove results. This was not the case before Google.cn established this practice with its launch in 2006.

Google's response to censorship efforts

Google works to ensure that our products serve as platforms for free expression, and we are deeply committed to making sure that our products remain vehicles for individual speech, collaboration, learning, and political participation.

To realize these aspirations, we are engaged in numerous activities to help promote free expression online.

Promoting transparency

Providing our users with transparency – an understanding of how our products work – is one of our core principles. In the context of government regulation of content, we try to provide transparency whenever we are required to remove content from our products.

To this end, when we remove content from our search results in response to a legal request, we send the request to Chilling Effects (www.chillingeffects.org), a joint project of the Electronic Frontier Foundation and several academic institutions including Harvard, Stanford, Berkeley, and the George Washington School of Law legal clinics, when we are able to do so legally. Chilling Effects posts the removal requests on its website, and we link to the publication of the complaint in place of the removed content. We are a leader in this level of transparency and the only major search engine to regularly and publicly disclose these removals.

In China, we take the following actions to promote transparency on the Google.cn search engine:

- First, whenever we offer censored results on our Google.cn search engine, we present clear notification on the results page to users. That notification states that, in accordance with local laws, regulations, and policies, we have not displayed all of the results in response to a query. In our view, there is value in letting our users in China know that the information that they searched for exists but cannot be made available because of limitations imposed by their government.

- Second, our Google.cn search engine sometimes shows results that, when clicked on, do not go anywhere because access to the destination site has been blocked. In those instances we show snippets of the blocked page so that, again, Chinese users can see that results have

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00150 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.111

been limited by their government's actions.

- We also provide a link to Google.com on the Google.cn home page, so that Chinese users know that there is an unfiltered alternative – at least to the extent that it is not being blocked.

Providing transparency for users is important because it tells them that, though they may not be able to access information, that information does exist and can be accessed through other means. Transparency allows users to make informed decisions about the services they choose to use.

Establishing best practices

One company alone can have only limited impact. In testimony before the U.S. Congress in 2006, we said that we would work with other technology and telecommunications companies to develop shared principles that can serve as guidelines for doing business in countries that restrict access to internet content and information.

To this end, Google has played an active part in efforts by a group of companies, human rights organizations, socially responsible investors, and academics to produce a set of principles to guide the response of companies when faced with laws, regulations, and policies that threaten free expression and improper government requests for access to personal information.

Our group has been meeting for more than 18 months and, although it hasn't always been easy, we are optimistic that we will reach an agreement not only on a set of principles but also on ways to demonstrate that companies are putting those principles into practice. Google has taken this process extremely seriously, with our employees investing hundreds of hours and exploring these topics with the senior leadership of the company.

We believe that this effort is consistent with our own current practice of conducting risk assessments that consider the impact on free expression and other human rights of entering new markets or introducing new products into existing markets. Our assessments balance our mission to provide information to citizens around the world with a need to protect our users as well as the safety of our employees around the world.

Collaborating with the human rights community

We also engage with human rights bloggers and other agents of free expression to help them use our products to promote more robust and more diverse speech online.

For example, we have worked with organizations such as Witness, Amnesty International, UNICEF, The Human Rights Foundation, The Equality and Human Rights Foundation, Human Rights First, and Human Rights Watch to start YouTube channels that give voice to human rights issues often ignored by the mainstream media. One of our human rights partners, Witness, uses videos to shed light on human rights abuses around the world.

You can see many of these organizations' channels and the videos they produce at a special human rights channel that we've created located at youtube.com/humanrightschannel.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00151 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.112

And we continue to underscore our commitment to human rights in our products themselves. For example, we have worked on several human rights projects with the United States Holocaust Museum. The museum's "World is Witness" project uses Google Earth and Blogger to document and map genocide and related crimes against humanity. The initial entries are from a recent Museum visit to Rwanda and the Democratic Republic of the Congo to learn about the legacies of Rwanda's 1994 genocide. And the museum's "Mapping the Holocaust" project uses Google Earth to map key Holocaust sites with historic content from its collections, powerfully illustrating the enormous scope and impact of the Holocaust.

Fighting censorship through technology

Finally, we continue to provide resources to support the development of technology designed to combat internet censorship. For example, we provide platforms where people can host anti-censorship projects free of charge, much in the same way that YouTube hosts videos and Blogger hosts blogs. For example, the developers of Gladder, a Firefox browser extension that is used to counter censorship, use our Google Code platform to host their project. In addition, Google provides development resources to TOR (The Onion Router), an anonymizing program that allows individuals to get around internet censorship technologies.

Supporting government efforts to promote free expression

Google's support for free expression initiatives

Internet censorship is a real challenge, and not one that any particular industry – much less any single company – can tackle on its own. Efforts to promote freedom of expression and to limit the impact of censorship require both private and public sector engagement.

To that end, Google has encouraged the U.S. government to make combating internet censorship a top priority. We believe that government-sponsored censorship is one of the largest barriers to providing more information online and more access to internet-based services – with serious implications for trade and human rights. It is vital for the U.S. Departments of State and Commerce and the Office of the U.S. Trade Representative – in this and in future administrations – to make censorship a central element of our bilateral and multilateral agendas.

In that vein, we applaud the U.S. government's efforts to date to promote the free flow of information in our trade agreements. In addition, the Department of State has helped promote freedom of expression on the internet. Among other things, the State Department has created the Global Internet Freedom Task Force, an internal departmental coordination group that addresses challenges to freedom of expression and the free flow of information on the internet. The State Department has been a strong advocate in United Nations summits and other forums for the right of all persons to create, access, utilize, and share information on the internet, subject only to limited restrictions for legitimate government purposes.

Google has been supportive of these efforts – but we believe that more must now be done.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00152 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.113

Recommendations for combating global internet censorship

As we approach the 60th anniversary of the signing of the Universal Declaration of Human Rights, we believe governments that embrace free expression should do more to ensure that the world community respects free speech in cyberspace. International agreements designed to ensure free expression – no matter the particular medium – exist and have been ratified by the U.S. and many, many other countries. However, more can be done to make sure that these agreements are effective and enforced.

The Universal Declaration resulted in the International Covenant on Civil and Political Rights, a U.N. treaty that entered into force over 30 years ago and is commonly known as the ICCPR. The ICCPR very clearly protects freedom of expression: "Everyone shall have the right to freedom of expression . . . to seek, receive and impart information and ideas of all kinds" through any medium. Recent interpretations of the ICCPR make clear that the internet is covered under the agreement.

However, not enough has been done to ensure that the ICCPR truly protects free expression online. We also believe that the U.S. government could act more aggressively to promote online freedom of expression.

We offer the following suggestions as ways of building upon existing human rights mechanisms to reinforce America's and the international community's commitment to free expression throughout the world.

- ***Promote the universal ratification of the International Covenant.*** Not every country that has signed the ICCPR has fully embraced its obligations by ratifying it. Approximately 30 countries are not parties to the agreement including China, Cuba, and Saudi Arabia. We would strongly recommend that the U.S. renew diplomatic efforts to encourage these countries to ratify the covenant, and to file separate declarations under the treaty to consent to the Human Rights Committee's jurisdiction over complaints by States against other States. We also believe that more governments – including the U.S. – should be encouraged to join the covenant's First Optional Protocol, which enables individuals to file complaints.

- ***Strengthen and enhance the State Department's Global Internet Freedom Taskforce.*** Much has been accomplished by the State Department's Global Internet Freedom Taskforce, but the initiative could be given increased prominence, authority, and funding. Increasing and enhancing the role of the taskforce could leave behind a strong legacy for the current Administration in the area of free expression online, and help ensure that promoting internet freedom is a central priority for the next Administration. Among other things, the agenda could be given increased prominence and authority by, for example, appointing an Ambassador-at-Large for Internet Freedom – which would be a position similar to the Ambassador-at-Large for International Religious Freedom.

- ***Support increased focus by the UN Human Rights Committee on Internet freedoms.*** In the area of internet censorship, the States Parties to the ICCPR could focus more attention on impediments to free expression online. For example, the Committee could issue a general comment addressing relevant articles in the Covenant and how they apply to internet restrictions.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00153 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.114

- ***Ensure that countries that are parties to the Covenant submit human rights reports enabling international review.*** The ICCPR requires States Parties to submit periodic reports on compliance with their ICCPR obligations – generally every four years – to the Human Rights Committee, which conducts a detailed review and issues an assessment of treaty compliance. Many governments have not complied with this requirement, and the United States itself was out of compliance until it submitted a report in late 2005. The U.S., now having fully embraced its reporting obligations, should work to ensure that States Parties file their reports on compliance with the ICCPR in a timely fashion. This may need to involve offers of support for developing countries who are daunted by the effort involved in drafting the reports and submitting them for review, but we believe that this would be a worthwhile investment that would help protect human rights around the world.

- ***Strengthen individuals' ability to file complaints under the International Covenant.*** The ICCPR enables individuals to file complaints with the Human Rights Committee. We believe that the governments that promote free expression could provide funding and other support to non-governmental organizations and other groups to assist individuals in filing such complaints, as well as increasing awareness among relevant populations of their rights under the ICCPR. In addition, participating governments could, through the U.N., provide additional funding that would enable the Committee to address more individual complaints in a timely way, as the Committee is now substantially underfunded.

- ***Explore methods of shining more light on violations of freedom of expression.*** We believe that more attention focused on instances of internet censorship will result in greater accountability and transparency and – ultimately – less censorship by governments. For these reasons we would urge the U.S. government to promote enhanced monitoring of instances of internet censorship by governments.

- ***Promote free expression as part of foreign aid.*** We believe that the U.S. government could use foreign aid and other programs to better promote ICCPR compliance and free expression on the internet. For instance, the government could incorporate internet freedom of expression into support for and assessments of good governance. In a related area, Google has already urged officials at the Millennium Challenge Corporation to incorporate internet censorship in measuring whether candidate countries have achieved criteria for democratic governance.

At the same time, we continue to urge governments to recognize that information restrictions on the internet have a trade dimension. We urge the U.S. government in particular to continue to use trade agreements and other trade tools to promote the free flow of information on the internet, and to seek binding commitments wherever possible.

The bottom line is that much, much more can be done by the U.S., and at the international level by countries that respect free expression online, to ensure that individuals, companies, and others can use the internet as the free and open platform that it was designed to be. We would be happy to assist the Subcommittee in exploring and helping to implement these and other expression-enhancing initiatives.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00154 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.115

Conclusion

I would like to conclude by thanking Chairman Durbin, Ranking Member Coburn, and the other members of the Human Rights Subcommittee for helping to highlight the importance of the internet to free expression around the world. It is only with the attention and involvement of leaders like yourselves that we can make real progress in the effort to combat censorship throughout the world.

We look forward to continuing to inform you about our speech-expanding products, our efforts to promote free expression, and our recommendations for policy makers in this very important category of basic human rights.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00155 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.116

STATEMENT OF
THE WORLD ORGANIZATION FOR HUMAN RIGHTS USA

PRESENTED TO
THE UNITED STATES SENATE COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON HUMAN RIGHTS AND THE LAW

MAY 20, 2008

**"GLOBAL INTERNET FREEDOM:
CORPORATE RESPONSIBILITY AND THE RULE OF LAW "**

The World Organization for Human Rights USA thanks Chairman Durbin for holding this hearing on Global Internet Freedom and corporate responsibility, and appreciates the opportunity to provide this statement. Human Rights USA has a special interest and unique ability to deal with issues associated with how U.S. companies (and the Congress) should address human rights and the Internet, as the only international human rights group focusing exclusively on U.S. compliance with human rights standards. Last year our group reached a major settlement agreement in a lawsuit we filed against Yahoo! challenging that company's practice of providing to the Government of China Internet user identification information for a substantial number of journalists like Shi Tao, as well as political dissidents, resulting in their arbitrary arrest, long-term detention and torture. Yahoo!'s substantial role in facilitating these human rights abuses was confirmed when the decisions issued by the Chinese courts condemning Shi Tao and others to jail cited Yahoo! numerous times as the principal source of the information that led to their prosecution. That case posed key issues regarding the role and accountability of U.S. companies in major human rights abuses taking place abroad, and our group's experiences in handling that case provides important insights into the justifications that U.S. companies give to explain why they should not be held accountable, even when their actions contribute significantly to major instances of repression and torture.

This written testimony is being presented to emphasize the urgent need to clarify and strengthen the legal standards applied to U.S. corporations doing business abroad, so that they more fully understand and accept their responsibility for assuring that their actions and conduct do not contribute in a significant way to major human rights abuses. Providing the names and contact information of dissidents to repressive regimes, as Yahoo! did, is only one way that U.S. corporations are participating in and supporting repression. Many other U.S. companies are providing the products, technology and training to repressive governments and their agents that allow these governments to carry out the surveillance and tracking activities that places journalists and others at risk simply because they choose to exercise their free press and free speech rights. Also, American investment firms and pension funds are investing in the foreign entities in China and elsewhere that carry out the abuses. In short, Americans are facilitating and financially supporting torture abroad and U.S. companies are not

45688.117

acknowledging or accepting responsibility for them. A great deal more has to be done to make clear U.S. corporate responsibility for major human rights abuses taking place abroad.

Human Rights and Global Online Freedom

As the internationally recognized framework for understanding all global freedoms, human rights law provides the only appropriate lens through which to identify obligations for protecting online freedoms. Many of the technologies discussed at today's hearing are simply new electronic tools for age-old repressive government practices. Chilling political discussion, preventing journalists from publishing reports, and persecuting dissident writers are hardly new problems. The only difference is that the Internet is now the most prevalent means of worldwide communication. The starting point of the discussion, therefore, should be the universal human rights norms that protect online communications and protect individuals from government abuse of information technology.

Though the Universal Declaration of Human Rights was written almost 60 years ago, the protections set out in that text are relevant to today's Internet communications. These rights include:

- Freedom from arbitrary interference with privacy or correspondence.
- Freedom of thought, conscience, and religion;
- Freedom of expression;
- The right to form and hold opinions;
- The right to seek, receive, and impart information and ideas through any media and regardless of frontiers;
- Freedom of peaceful assembly and association; and
- The right to education.

These same rights are enshrined in numerous international treaties, including the International Covenant on Civil and Political Rights, which the U.S. Senate has ratified. Furthermore, these rights are considered customary international law, which are legal obligations that all nations must uphold.

Violations of Human Rights Using Information and Communications Technology: Denying Access, Censorship, and Surveillance

Repressive governments violate these fundamental human rights online in three ways: (1) unlawfully limiting access by individuals to the Internet, (2) censoring information available online, and (3) abusing the Internet infrastructure and other communications networks as a surveillance tool.

- Access restrictions include the types of extreme filtering systems used by Saudi Arabia and Iran to prevent their citizens from accessing any information that has not been approved by the government. Government-imposed filters

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00157 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.118

on the Internet violate the rights of users to seek and receive information and to form political opinions.

- Censorship can take many forms. Search engines may block results that include unapproved terms, blogging software may prevent users from posting specific terms and phrases, or online news sites may be ordered to remove critical articles. A government may also create arbitrary laws that chill speech and lead to "self-censorship" of the media and individual writers. Censorship thus violates the rights to freedom of expression, freedom to form a political opinion, freedom to seek, receive, and impart information, and the right to an education, among others.

- The most well-known online human rights violations – arbitrary imprisonment of journalists for the contents of their emails – result from surveillance, but there are other examples that may be more pervasive. Police and intelligence technologies that analyze voice patterns, scan faces in crowds, or track the locations of mobile phone users, present frightening scenarios for human rights defenders, journalists, and anyone who dares question government actions. This kind of invasive surveillance violates the right to privacy, as well as the right to freedom of thought and the right to free expression. It also deters individuals from asserting all of their inherent freedoms protected under international human rights law. Surveillance is the most insidious of the three abuses because it often leads to the violations of physical integrity: arbitrary arrest, arbitrary prolonged detention, and torture.

Corporate Responsibility for Respecting, Protecting, and Advancing Human Rights

The moment a corporation provides a government with the technology for filtering, censoring, or monitoring, the company becomes entangled in these human rights violations. And yet, information and communications technology companies are not facing this reality, nor are they accepting their responsibilities. As institutions of society and as citizens of the world, corporations have responsibilities to respect, protect, and advance recognized human rights norms. Because these norms are universal, they apply everywhere a transnational corporation operates.

Companies cannot trumpet their accomplishments to advance certain human rights, while at the same time actively undermining others. And yet this is precisely what some of the corporations you will hear from today have said under oath in previous testimony before Congress and in their annual reports to shareholders. They will claim that they must follow the laws of the countries in which they do business, without acknowledging that they are aiding and abetting those countries to violate international human rights laws. They will say that the people of repressive countries are better off having American companies provide them with the infrastructure for freedom of expression, and that the advances their products and services provide justify the "corners they have to cut." This argument disregards the legal obligations that

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00158 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.119

corporations have to uphold all fundamental human rights, not just some. The advances achieved cannot be sustained without a comprehensive approach to protecting human rights in all aspects of Internet communications. Corporate officers must ask themselves: Are my business practices actively entangling the corporation in human rights abuses? Is my company providing the tools of oppression to a foreign government? If the answer is yes, then the company is knowingly supporting violations of international law and bringing legal liability for that assistance onto the corporation and its officers.

As with any law, there will always be lawbreakers. We are too well aware that all nations do not observe these laws at all times. But no government in the world openly rejects the human rights standards enumerated above. Repressive governments always claim to honor these values, but carve out broad exceptions for "special circumstances" like national security and apply them arbitrarily to anyone who would assert their rights. In these situations, law-abiding nations should use the foreign policy tools at their disposal to influence and enforce international human rights in countries that are not fulfilling their own obligations to their citizens and the world.

Thus it falls to the United States to lead the way in enforcing global Internet freedoms. As the world's innovator in developing Internet technologies, the United States has a special opportunity to accomplish this. And yet, many of the corporations that provide repressive regimes with the technological infrastructure to carry out human rights violations are headquartered within our borders. Congress should look very carefully at the human rights laws it has already passed to see whether they are being observed, as well as the need for new laws. For example, the Electronic Communications Privacy Act, 18 U.S.C. § 2511, prohibits Internet service providers from disclosing their users' communications. Although there is an exception in this law for requests by law enforcement agencies, they must be reasonable requests that do not abuse the powers of the law enforcement official making the request. Thus responses to demands for information from foreign law enforcement agencies when that country's laws do not provide due process protections covering the communication would violate the ECPA.

Existing laws also prevent the sales of Internet surveillance devices. Congress adopted the Tiananmen Square Export Prohibitions, P.L. 101-246 §902(a)(4), and the Leahy Amendment, 22 U.S.C. § 2304(a)(2), to prohibit American companies from putting the tools of oppression into the hands of foreign police departments known to carry out major human rights abuses. Another section of the ECPA, 18 U.S.C. § 2512, prohibits the manufacture and sale of devices for intercepting electronic communications, which would seem to prohibit routers and other Internet infrastructure hardware, as well as surveillance software, that some companies are selling to police agencies in China and other countries known to intercept emails as a way of targeting dissidents. Yet evidence continues to surface that U.S. corporations are marketing and transferring advanced surveillance technologies directly to known human rights violators.

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00159 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.120

Conclusion

This Subcommittee should thoroughly investigate violations of binding international laws and existing federal laws regarding human rights and the Internet, and the responsibility of U.S. corporations to not be complicit in repression in countries where they do business. It also should look carefully at the Executive Branch's failure to enforce existing laws on these matters, and support the adoption of new laws to strengthen U.S. compliance with human rights standards in the way U.S. companies do business abroad.

Morton Sklar
Theresa Harris
World Organization for Human Rights USA
2029 P Street, N.W., Suite 301
Washington, D.C. 20036
(202) 296-5702
http://humanrightsusa.org

VerDate Aug 31 2005 11:59 Dec 10, 2008 Jkt 045688 PO 00000 Frm 00160 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\45688.TXT SJUD1 PsN: CMORC

45688.121

Senate Committee on the Judiciary
Subcommittee on Human Rights and the Law

Hearing on Global Internet Freedom: Corporate Responsibility and the Rule of Law
May 20, 2008

Testimony by Shiyu Zhou, Ph.D.
Deputy Director, Global Internet Freedom Consortium

Mr. Chairman, members of the Committee, Ladies and Gentlemen. I would like to thank you for this opportunity to testify before you today on the topic of global Internet freedom and the Corporate Responsibility and the Rule of Law.

The lack of information freedom in closed societies is usually coupled with severe violations of human rights and it also puts the United States at risk. In Iran, Cuba and certain other totalitarian countries, information control is often used for manipulation and indoctrination and whipping up anti-US sentiment, as illustrated by the xenophobia fostered online in the People's Republic of China (PRC) following the Tibet crackdown and the Olympics Torch Relay. Violence begins with hate, and hate begins with distorted information.

Information control can also cost lives. When the PRC leadership chose to suppress news of the SARS outbreak in 2002, the virus spread far beyond China's borders to places like San Francisco, causing the death of at least several hundred victims and almost a global pandemic.

The Internet has become the greatest hope for global information freedom. It is a vast, fast, and inexpensive way to access information and to communicate and the number of Internet users worldwide has soared. By January of this year, the PRC had 210 million users and has since surpassed the US, and both Iran and Vietnam were at 18 million users and growing. While authorities in closed societies can easily shut down newspapers, block TV channels, jam short-wave radios, and ban books, the Internet is far more elusive. With the proper anti-censorship technologies, users in these societies can access uncensored information online freely and without fear of reprisal. Anti-censorship is sometimes called anti-blocking or anti-jamming and refers to technical means that protect users in closed societies from being monitored, blocked, or tracked.

For more and more users around the world, that proper anti-censorship technology means tools like FreeGate and UltraSurf -- created by the Global Internet Freedom Consortium (GIF), a small team of dedicated men and women, connected through their common practice of Falun Gong, who have come together to battle tens of thousands of Internet monitors and censors around the world to work for the cause of Internet freedom. I am proud to stand before you today on behalf of this illustrious group because I feel they are truly heroic. They have allowed millions of citizens inside repressive societies to experience the Internet as we in free societies experience it – being able to use Wikipedia to look up a new word or post a blog without having to look over

45688.122

their shoulders. The Consortium provides its products and support services to those citizens entirely free of charge.

The companies and organizations that make up the Consortium have maintained the world's largest anti-censorship operation since 2000. The focus was originally on the PRC as China's censorship measures on the Internet are by far the most sophisticated and extensive among all the closed societies. As more and more nations have followed China's lead, however, our experience has made us uniquely equipped to help advance Internet freedom around the globe. Outside of China, the second largest segment of our user base is now in the Middle East: in Iran, Saudi Arabia, United Arab Emirates, and Syria.

Of the 43 countries identified as "Not Free" in Freedom House's *Freedom of the Press 2008 Survey*, GIF's anti-censorship systems have served users in the following 33 countries as of January 2008: Algeria, Angola, Azerbaijan, Belarus, Brunei, Burma, Cambodia, Cameroon, China, Congo, Cote d'Ivoire, Cuba, Egypt, Iran, Iraq, Kazakhstan, Laos, Libya, Maldives, Oman, Pakistan, Qatar, Russia, Rwanda, Saudi Arabia, Sudan, Syria, Tunisia, United Arab Emirates, Uzbekistan, Vietnam, and Zimbabwe.

Our five existing tools – UltraSurf, DynaWeb FreeGate, Garden, GPass, and FirePhoenix — currently accommodate an estimated 95% of the total anti-censorship traffic in closed societies around the world, and are used **DAILY** by millions of users. These tools have been of benefit to US-based organizations such as Human Rights In China, the Chinese Democracy Party, Voice of America, and Radio Free Asia -- and even companies like Google and Yahoo since we bring the uncensored version of their services into closed societies like China.

As of January 2008, the Top Five censoring countries with the most average daily hits to our anti-censorship systems are (hits per day):

(a) China:	194.4 million
(b) Iran:	74.8 million
(c) Saudi Arabia:	8.4 million
(d) UAE:	8 million
(e) Syria:	2.8 million

Clearly, besides China, a significant portion of the user base is from the Middle East.

We have witnessed first-hand the effectiveness of anti-censorship technologies in improving information freedom for people in closed societies. During the democratic movement in Burma in late August 2007, our anti-censorship portals were receiving over 120,000 average hits from IP addresses originating inside Burma every day; a three-fold increase from less than 40,000 prior. That number has since more than doubled in the wake of the cyclone.

After the protests broke out in Tibet on March 10 of this year, there was a four-fold increase in the number of daily hits to our anti-censorship portals from Tibet, from the daily average of 120,000 before March 10 to about 480,000 after March 10. The daily number of hits reached more than 800,000 on March 16. The measures Chinese authorities have taken to clamp down on

45688.123

information going in and out of Tibet are severe. The Consortium's anti-censorship tools are now one of the Tibetans' few remaining links to the outside world.

A particularly insidious aspect to information control is that it allows a repressive government to spoon feed the populace with whatever false information it chooses. In closed societies such as China and Iran, censorship is used by the leadership to save face, deflect criticism, and turn domestic discontent against external enemies both real and imagined. A few carefully edited TV news segments, a few doctored articles in the newspapers, a few carefully placed key words to dehumanize the target, and the result is a very large and very hostile population. The US would do well to heed the very real threat this poses to our national security.

Internet freedom is one of the most effective ways to allow the US to win the hearts of the people in closed societies, and its young people in particular, and to help move the world in more benign and realistic directions. Anti-censorship technology can allow the people in closed societies to be better informed and to be less subject to manipulation by an unscrupulous leadership. Winning people over to a more open and free system via the Internet could very well be a way to avoid damage and loss of life in future conflicts. It is no exaggeration to say that an online information battle, if fought well, could ultimately help to prevent a real war.

It is thus not surprising that China maintains an Internet "firewall" bureaucracy of over 30,000 officials and that, as reported by the State Department/Foreign Operations Appropriations Committees, Chinese President Hu Jintao has spoken of a crisis involving "the stability of the socialist state" that will only be cured if the Internet can be "purified."

In the on-going struggle between the censors and anti-censorship efforts, it is crucially important to stay ahead of the game. Repressive regimes have been spending enormous sums on developing censorship tools in recent years. We should also be aware that China's military is actively developing sophisticated ways to wage digital warfare against America. For years, Chinese authorities have indoctrinated "patriotic hackers" to infiltrate and take down US government computer systems. Just recently, these hackers were instigated to attack the CNN website en masse. If the US does not maintain its current lead in anti-censorship technologies over censors now, there could be a much higher price to pay down the road.

Our statistical data show that currently Chinese elites are among the most avid users of our anti-censorship services, for they want to know what is happening in the world that their government does not provide them. It has been transforming the Chinese society in a peaceful but powerful way that must not be underestimated. ***Once a critical mass, 10 percent we believe, of the 230 million Internet users in China get to know the existence of our anti-censorship tools and, especially, gain a positive experience of using them, the avalanche effect of such a development will in our view lead to the fall of the Beijing censorship Wall and, consequently, to the fall of other Walls in the world's other closed societies.*** Imagine, then, the possibilities of the Pope being able to conduct an interactive worship service with millions of House Church Chinese Catholics, or Members of this Committee being able to conduct seminars in democracy with tens of thousands of Iranian students -- all without fear of detection or arrest using our scaled-up services.

45688.124

The battle of Internet freedom is now boiling down to the battle of resources. ***It is our belief that $50 million – enough to allow GIF programs to scale up their operations through purchasing equipment and expanding network capacity - will be enough for us to reach the critical mass of 10 percent of the 230 million Internet users in China.*** Importantly, the time for doing so is this coming year, given the current political dynamic in China and the upcoming Olympics. We hope and trust the Senate and the Congress will grasp what we believe to be a historic opportunity.

Only when the US shows more determination to keep the Internet open than the closed societies are showing to seal it off, can there be the hope of information freedom and democracy for the citizens in all closed societies, and a more peaceful tomorrow for mankind.

We would like to thank Senator Leahy, Senator McConnell, Senator Gregg, Congresswoman Lowey, Congresswoman Ros-Lehtinen, Congressman Wolf, Congressman Berman, and other members of Congress, and Ambassador Mark Palmer of Freedom House, Michael Horowitz of Hudson Institute, former Director of NTIA Clay Whitehead, and Human Rights Watch DC Office Head Tom Malinowski, for the support they have provided my colleagues. In particular, we thank Senator Leahy, Senator McConnell, Senator Gregg, Congresswoman Lowey, and Congressman Wolf, for the Internet freedom initiative in the fiscal year 2008 Foreign Operations Appropriations Bill which set up a competition for a $15 million grant for "field-tested" Internet technology programs and protocols that, in the words of the appropriation legislation, "have the capacity to support large numbers of users simultaneously in a hostile internet environment."

Below is a more detailed description of the current state of Internet censorship around the world, how people have benefited from the services we've been providing, and how our services might be expanded to successfully tear down Firewalls in closed societies around the world.

The State of Internet Censorship

A number of countries actively censor the Internet, including Iran, the People's Republic of China, Burma, Saudi Arabia, and Vietnam. Since China's censorship measures on the Internet are by far the most sophisticated and extensive and are emulated by many other nations, the state of Internet censorship in China illustrates well the nature of the problem in other closed societies.

Since 1999, we have seen China's Internet censorship capability evolve from rudimentary measures to systematic and highly advanced technological deployments. Those of us who have worked for the world's top technology companies can tell that the capability and sophistication of the Chinese government's censorship technology is at such a level that they are using the most top-of-the-line, cutting-edge products.

Today there are three mechanisms at work on the Great Firewall. One is Internet Protocol Address blocking, or **IP address blocking**. An IP address on the web is like a phone number on a telephone network. IP address blocking is simply denying your visit to overseas websites with certain IP addresses. The websites targeted by the censors are mostly about Falun Gong, the Tiananmen Square massacre, Tibet, Taiwan, human rights, etc.

45688.125

The second mechanism is called **content filtering**. Chinese authorities have built powerful net machinery to sniff all the net traffic going through the Great Firewall in either direction. Once they detect a keyword in the traffic, they will simply cut off that particular traffic flow. The user ends up staring at a blank screen as though he has suddenly lost his Internet connection. This method indiscriminately blocks access to any site that happens to have one of the keywords included on the long official list.

The third mechanism is the most malicious – we call it **Domain Name Redirect**. This method can be likened to publishing a phone book with the number of the people you dislike changed to other numbers so no one will ever be able to reach these people. Another analogy would be changing all the street signs so no one knows where they are actually going. This is a flagrant violation of international Internet conventions and standards on a national-scale, but apparently the censors do not feel any obligation to play by the rules when they want to control information.

Besides the technological aspect, there is a whole other dimension to censorship on the Net. We call it the "human flesh Great Firewall." At the top is an army of tens of thousands of net police patrolling the web space in China. Down below are countless website administrators who are forced to sift through the blogs, forums, and bulletin boards they are managing to delete any posts deemed "sensitive" according to certain arbitrary rules. In addition, Internet service providers (ISPs) are told to keep an eye on the sites they are hosting and be ready to shut down the sites that cross another arbitrary line drawn by the state. Internet content providers such as search engines and portal sites also devote significant time and effort in preemptive self-censorship.

Demand and Impact of Anti-censorship Services

Since the early days of the censorship, we have been providing censorship-circumvention service to users living in oppressive regimes. We started as a few independent and scattered groups, including Dynamic Internet Technology, Inc. (DIT), UltraReach Internet Corporation, Garden Networks for Freedom of Information Inc., World's Gate, Inc., and Global Information Freedom, Inc. Each group had a different technical approach.

Our services were originally targeted towards and promoted to Internet users in China, but over time we have also attracted a large number of users from other closed societies, such as Iran, Burma, and Saudi Arabia.

In 2006, these groups formed a consortium, Global Information Freedom Consortium to pool their experience, infrastructure, resources, and technological talents together. The purpose was to provide better service to users and beat censorship more effectively, especially when each of the groups had limited resources.

Our anti-censorship services were developed and evolved in response to two major user demands: **to surf the web freely and securely and to post information on the websites inside China without exposing the identity and origin of the connection**. Our services have three major facets:

45688.126

1. **Anti-censorship tools:** These are a variety of software tools we provide to users to defeat blocking, monitoring and tracing of their online information and activities. When a user in China fires up our system, the bits and bytes flowing in and out of his/her computer are scrambled, so the Great Firewall cannot see any patterns in the traffic and therefore has no idea if it detects something suspicious or not. Additionally, our tools are highly dynamic and know where the cracks in the Great Firewall are. The tool changes its network connection from time to time to avoid becoming a sitting duck.

   Currently we have five major tools from our coalition to cater to our users' demands, including DIT's **FreeGate**, UltraReach's **UltraSurf**, Garden Networks' **Garden**, and World's Gate's **GPass** and **FirePhoenix**. They have different features and technical strengths and they are also constantly evolving in response to the ever-changing censorship technologies.

   The variety of our tools provides our users with a real edge. They have reported that with such a selection, they are almost unstoppable. Whenever one of our tools is jammed by the censors, a user can switch to another tool to either get back online or download a newer version of the jammed one. Such a complementary nature seems to greatly enhance the users' confidence in our offerings.

2. **Infrastructure:** Once a user launches one of our tools, information is relayed to a network we have built in free countries, mostly in the U.S. This network is like an Underground Railroad in cyberspace, but much more dynamic. The capacity of this infrastructure directly impacts the number of users we can support.

   This network also provides extra services. For example, World's Gate provides low-cost web-hosting services to users in closed societies so they can enjoy freedom of expression by establishing forums, discussion groups, etc. on our network in addition to the native support of censorship-resistance.

3. **Promotion and user support:** We have found it is critical to perform user outreach, because the news about the availability of our services is itself blocked. Therefore we have to actively spread the word via the Internet using emails, instant messages, forum posts, and traditional means such as long-distance telephone calls and postal mail. Once the user base reaches a critical mass, it becomes much easier because the news can be spread through word-of-mouth.

   Timely technical support for users is a must for a successful anti-censorship system. Our five systems (FreeGate, UltraSurf, Garden, GPass and FirePhoenix) are now sharing a unified technical support platform, www.qxbbs.org, in which each system has its own user forum. It is a place where users can share their experiences and developers can provide technical support. For example, there are more than 20,000 posts on DynaWeb's support forum with information ranging from technical tips to compliments from users to reports from China of new blocking test results. This operational area also includes internationalization, i.e., translation of user interface, documentation and instructions into users' native languages.

45688.127

Currently the Consortium is running the largest anti-censorship operation serving 95% of the circumvention traffic from about 2 million users.

Our services are not limited to Chinese users. Within two days in January, 2008, we witnessed on our system users from 33 out of the 43 countries identified as "Not Free" by Freedom House's Freedom of the Press 2008 Survey, GPass has become a favorite with Iranians ever since it released a Farsi (Persian) version.

Our services have also benefited US-based organizations such as HRIC, the Chinese Democracy Party, VOA, and RFA.

Our Challenges

As a grassroots organization, we feel we have been fighting against a Goliath in cyberspace alone. Challenges we have been facing include:

1. **Censors using high-tech equipment with ever-increasing performance for Internet snooping and control.** The intelligence of our adversary, as well as our own system, learns and evolves with time and with experience, and with high-end machinery.

   Although we have not physically seen the machines in the server room of those in charge of maintaining the Chinese Firewall, the advanced capabilities indicate they constantly upgrade their hardware with top-of-the-line items on the market.

2. **Resource limitations**. So far our endeavor has been sustained mostly by volunteers. On the one hand, more and more users are eager to get on our Underground Railroad; on the other hand, we have limited bandwidth, hardware, manpower, and time to expand and satisfy their needs.

   I believe we have the most advanced anti-censorship technologies around. That is why we are ahead of the game most of the time, and why we have been able to support an ever-increasing user base. But technology is not the only determining factor. The game is now boiling down to a battle of resources. Besides the hardware of the Great Firewall, the censors have also assembled an army of tens of thousands of net police to serve as a human flesh Great Firewall. That is a challenge for us because our current resources make it difficult if not near-impossible to match that kind of manpower. On the other hand, our experience indicates every penny we invest in our offense will force the censors to burn a dollar or more in defense. So every penny counts a lot in our effort.

3. **Attacks from all directions**. The Chinese Communist Party (CCP) has no interest in playing a fair cat-and-mouse game on the Internet. It constantly launches cyber attacks on our infrastructure and our people. Attempts to hack our websites are non-stop, emails impersonating our own people with virus attachments are abundant, harassing phone calls are not rare events. It even resorted to physical violence on U.S. soil when other measures

45688.128

failed: Armed Asian men broke into the home of the president of our organization, Yuan Li, in Atlanta, brutally beat him and stole his computers while leaving other valuables intact. We have reason to believe the CCP was behind the attacks.

As a side note, we would also like to point out that it seems the CCP has been using our systems as practice targets before it launches attacks against US and other countries' government networks. The tactics used in these attacks share much similarity with what we have seen.

Besides the direct attacks, the Chinese regime has also forced anti-virus companies in China to identify our software tools as viruses to discourage users from adopting the software. Surprisingly, anti-virus companies in the US such as Symantec and Norton do not seem to want to be left behind as their anti-virus software also indiscriminately labels some of our tools as viruses. Our written clarification with them has fallen on deaf ears.

Despite all the difficulties, we have not wavered from our mission. Many of us have witnessed first-hand the Communists' brainwashing, hatred induction, and indoctrination, and we treasure the information freedom outside the Great Firewall. However, the people still confined within the Great Firewall need much more help. We urge government agencies, NGOs, and corporations to step in and contribute to these efforts.

For democratic governments, many actions can be taken to bring the anti-censorship endeavor to the next level. For example:

Provide resources to these efforts. This is the most effective support. Since anti-censorship technologies have matured and have been field-tested, most resources are now devoted to the operation of these systems instead of to research and development. The impact of such support would be immediately visible. The government should measure its achievements by not only the number of political prisoners released, but also the number of users who are enabled and empowered to access information freely.

Limit technology exports to repressive regimes. Evidence shows that the advanced Internet filtering technologies used in the Chinese Great Firewall are provided by Western companies. Democratic nations should impose restrictions on such exports as they can be exploited for future enhancements of the Firewall.

Establish a funding vehicle to rally financial and resource support from other organizations and corporations. In particular, those multi-national technology companies such as Yahoo! and Google that have said it is not "convenient" for them to provide an uncensored web to users in China could contribute to our efforts and we would be happy to step in.

The United States funded the creation of Internet a few decades ago. Now the Internet is used in repressive regimes as a powerful tool to suppress freedom and is being morphed into a dark weapon for cyber war targeting the US and other free nations. Please allow us to submit our humble opinion that defending the transparency and freedom of the Internet is of critical national

45688.129

interest and we believe the US government has a responsibility to play a much more active role in this endeavor.

****

The Roles of US Companies in China's Internet Censorship

There is unfortunately strong indication that companies in free societies such as Cisco may have involved in assisting the Chinese security services to monitor and censor the Internet, and persecute and prosecute Chinese citizens who just want to use Internet to access uncensored information and/or express their own views freely and peacefully.

In a 2002 Cisco (China) PowerPoint presentation entitled "An Overview on [China's] Public Security Industry," now in our possession, a Cisco (China) official in the Government Business Department listed the "Golden Shield Project" – the host project of China's Great Firewall – as one of Cisco's major target customers. One of the main objectives in that Project, defined in the Cisco document as the "Monitoring and Control System for Public Internet Information Security," was to "combat the 'Falun Gong' evil cult."

We must take note that the two words of evil cult, the rhetoric of the Chinese Communist Party to persecute Falun Gong, are not even quotation-marked in the presentation. The view taken of my fellow-practitioners in the PowerPoint document raises obvious and profound concerns about Cisco's culpability in an Internet monitoring and censorship regime that has diminished freedom, added to the power of a powerful dictatorship and, in pursuit of those goals, caused the arrest and frequent murder of innocents at the hands of China's Firewall bureaucracy.

In the following PowerPoint page headed "Cisco Opportunity [on the Golden Shield Project]," Cisco listed the following four areas of potential assistance to China/business opportunities:

"* High start-point planning;
"* High standard construction;
"* Technical training; and
"* Security and operation maintenance."

The above areas of potential assistance appear to flatly rebut Cisco's repeated and self-serving claims that it has merely sold routers and other equipment to China's security services and has not in any way assisted or participated in the Internet censorship and monitoring activities of those security services.

In the battle between our Consortium and the totalitarian Chinese authorities, it appears that Cisco is selling router equipment to the Chinese police authorities by offering censorship training and other supports. Our research shows that the main Internet censorship of China involves IP blocking, content filtering and connection reset, and DNS hijacking, and they are all done at the national gateway level. The infrastructure of China's Great Firewall shown by our research coincides with the layouts in Cisco (China)'s PowerPoint document.

45688.130

We must appeal to these US corporations to reconsider what they are doing. Every time our anti-censorship tools are attacked using their technology, they are taking the side of the totalitarian authorities against Chinese people seeking some of the most basic of human rights. They are jeopardizing U.S. national security interests by directly compromising the safety of millions of Internet users in closed societies around the world. This is no longer just a virtual game, and it is certainly no longer just about dollars and cents. Real lives are at stake. Just ask Yahoo! how Mr. Shi Tao is faring as a prisoner of conscience facing several more years in his prison sentence for sending an email.

Our Consortium has been able to stay ahead of the censorship game by developing new software and new technology, but each battle has been grueling and certainly taps into our already scarce resources. Sometimes we feel like a little David fighting a constant battle with a monolithic Goliath out in cyberspace. It has been a lonely battle thus far and we are tired of having to fight our fellow American companies.

We intend to further investigate the history, use and meaning of the PowerPoint document, and to investigate all forms of assistance that Cisco officials may have given to China's Firewall and police bureaucracies in the latter's determined efforts suppress free Internet use and to brutally punish users and facilitators of uncensored Internet access. We call on Cisco to determine, on the basis of a thorough and searching investigation, the manner and extent to which the PowerPoint document was used and circulated within Cisco (China) and the extent to which the document's views were shared within Cisco (China). (We would like to know what the reaction of Cisco (China) officials was to the document's characterization of Falun Gong as evil.) We call on Cisco officials to acknowledge, immediately, once and for all and, at a minimum, that they can no longer assure Congress that Cisco (China) is and has been a merely passive seller of routers and other equipment to China's security services, and we further call on senior Cisco management to acknowledge that they can no longer assure Congress that Cisco (China) has not been and is not now an accomplice and partner in China's Internet repression and, whether directly or indirectly, its infamous "610 Office" persecution of Falun Gong practitioners in China.

A cloud of suspicion now hangs over Cisco, which self-serving assertions of innocence can no longer dispel. Nothing but the most thorough and independent investigation, which we hope will be closely monitored by this Committee, will remove the concern that, in its efforts to sell routers and other equipment to China's security police, Cisco (China) officials were complicit in the persecution of those who bravely work to end China's efforts to monopolize the free flow of information to, from and between its people.

We conclude by noting another form of censorship, namely, self-censorship by content providers or websites operators. International companies doing business in censorship countries, such as China, restrict themselves and provide tailored content to users in these regimes. A prime example is Google's Chinese version, which provides drastically different search results for queries originating in China from its versions in other locations. As a U.S. company that appears not to be aligned with the repressive forces in China, Google's collusion and collaboration with the repressive weapons of censorship make the efforts of those seeking to expose the Chinese people to the market place of ideas all the more difficult. Unfortunately, there exist no effective technical measures to overcome this form of censorship.

45688.131

So far the public have learned about Google's self-censorship mainly through media reports and rights organizations. Google itself has been silent about it. We believe that all Google users and shareholders deserve to know exactly what Google does to the 230 million Chinese Internet users. We therefore created the "Google Search Review" service, http://gg.edoors.com, that compares search results from google.com and google.cn.

We would like to offer the code to this Committee and to Google, and we respectfully request Google to host this service on their servers, and announce it to the public.

ADDITIONAL STATEMENT
SHIYU ZHOU
Senate Judiciary Subcommittee on Human Rights and the Law
Global Internet Freedom Hearing

Submitted documents reveal that Cisco has helped the public security police in China build the Golden Shield Project. The daily operation of the Golden Shield Project can be outsourced to ISPs by the public security police, but can also be done within some department of the public security. All ISPs in China are under the control of public security police, including ISPs at the national gateway level and at all local levels. Ultimately, Cisco provides the initial technical training and support.

ISP identifying users for police is only a small part of the Internet censorship. The majority of censorship takes place at the national gateway level, which controls what Chinese people can and cannot see on the Internet. This is the censorship that affects the most web surfers all the time.

The national gateway machinery also has the capability to track down users, especially when it joins hands with local ISPs. It can easily figure out the users who want to visit www.voa.gov, for example. The ISP at the national gateway is also under the control of public security police just the same.

Online documents reveal that the Golden Shield Project also uses Cisco solutions to do audio and video monitoring and surveillance, which can be extended to voice and image recognition using software.

45688.132