

GLOBAL INTERNET FREEDOM AND THE RULE OF LAW, PART II

HEARING

BEFORE THE
SUBCOMMITTEE ON HUMAN RIGHTS AND THE LAW
OF THE
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE
ONE HUNDRED ELEVENTH CONGRESS
SECOND SESSION

MARCH 2, 2010

Serial No. J-111-77

Printed for the use of the Committee on the Judiciary



GLOBAL INTERNET FREEDOM AND THE RULE OF LAW, PART II

GLOBAL INTERNET FREEDOM AND THE RULE OF LAW, PART II

HEARING BEFORE THE SUBCOMMITTEE ON HUMAN RIGHTS AND THE LAW OF THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ONE HUNDRED ELEVENTH CONGRESS SECOND SESSION

MARCH 2, 2010

Serial No. J-111-77

Printed for the use of the Committee on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE

61-829 PDF

WASHINGTON : 2010

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

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin	JEFF SESSIONS, Alabama
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
RUSSELL D. FEINGOLD, Wisconsin	CHARLES E. GRASSLEY, Iowa
CHARLES E. SCHUMER, New York	JON KYL, Arizona
RICHARD J. DURBIN, Illinois	LINDSEY GRAHAM, South Carolina
BENJAMIN L. CARDIN, Maryland	JOHN CORNYN, Texas
SHELDON WHITEHOUSE, Rhode Island	TOM COBURN, Oklahoma
AMY KLOBUCHAR, Minnesota	
EDWARD E. KAUFMAN, Delaware	
ARLEN SPECTER, Pennsylvania	
AL FRANKEN, Minnesota	

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MATT MINER, *Republican Chief Counsel*

SUBCOMMITTEE ON HUMAN RIGHTS AND THE LAW

RICHARD J. DURBIN, Illinois, *Chairman*

RICHARD J. DURBIN, Illinois	TOM COBURN, Oklahoma
RUSSELL D. FEINGOLD, Wisconsin	LINDSEY GRAHAM, South Carolina
BENJAMIN L. CARDIN, Maryland	JOHN CORNYN, Texas
EDWARD E. KAUFMAN, Delaware	
ARLEN SPECTER, Pennsylvania	

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

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Coburn, Hon. Tom, a U.S. Senator from the State of Oklahoma	3
Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois	1
prepared statement and attachments	34
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont, prepared statement	245

WITNESSES

MacKinnon, Rebecca, Visiting Fellow at the Center for Information Technology Policy, Princeton University, Princeton, New Jersey, and Co-Founder, Global Voices Online	23
Memarian, Omid, Iranian Blogger, San Francisco, California	24
Posner, Michael H., Assistant Secretary for Democracy, Human Rights, and Labor, Department of State, Washington, DC	4
Weitzner, Daniel J., Associate Administrator for the Office of Policy Analysis and Development, National Telecommunications and Information Administration, Department of Commerce, Washington, DC	6
Wong, Nicole, Vice President and Deputy General Counsel, Google Inc., Mountain View, California	21

SUBMISSIONS FOR THE RECORD

Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois, letters to Tech Companies:	
February 2, 2010, letter Regarding Internet Freedom in China	39
Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois and Hon. Tom Coburn, a U.S. Senator from the State of Oklahoma, joint letters to Tech Companies:	
August 7, 2010, letter Human Rights Code of Conduct	46
Responses to January 29, 2010 letter:	
Acer Incorporated, Lydia Wu, General Counsel, Taiwan, R.O.C., March 1, 2010 letter and attachments	49
Amazon.com, Paul Misener, Vice President, Global Public Policy, Seattle, Washington, February 18, 2010 letter	66
Apple Incorporated, Bruce Sewell, Senior Vice President & General Counsel, February 19, 2010 letter	68
AT&T, Timothy P. McKone, Executive Vice President, Federal Relations, Washington, February 18, 2010 letter	70
Cisco Systems, Incorporated, Mark Chandler, Senior Vice President and General Counsel, February 19, 2010 letter	72
Dell Incorporated, Gilbert F. Casellas, Vice President Corporate Responsibility, February 18, 2010 letter	75
eBay, John Donahoe, President and Chief Executive Officer, San Jose, California, February 18, 2010 letter	78
Facebook, Timothy Sparapani, Director, Public Policy, Palo Alto, California, February 19, 2010 letter	80
Fortinet, Incorporated, John Whittle, Vice President, General Counsel, Sunnyvale, California, February 19, 2010 letter	83
Hewlett-Packard Company, Larry Irving, Vice President, Global Government Affairs, Washington, DC, February 19, 2010 letter	85
IBM, Christopher A. Padilla, Vice President, Governmental Programs, Washington, DC, February 19, 2010 letter	91

(III)

	Page
Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois and Hon. Tom Coburn, a U.S. Senator from the State of Oklahoma, joint letters to Tech Companies—Continued	
Lenovo, Rachel A. Adams, Vice President and Assistant General Counsel, Washington, DC, February 19, 2010 letter	93
Motorola, Karen P. Tandy, Senior Vice President, Public Affairs and Communications, Schaumburg, Illinois, February 15, 2010 letter	95
MySpace.com, Rupert Murdoch, Chairman and Chief Executive Officer, New York, New York, February 18, 2010 letter	97
Nokia, Olli-Pekka Kallasvuori, President and Chief Executive Officer, Helsinki, Finland, February 23, 2010	99
Nokia Siemens Networks, Rajeev Suri, Chief Executive Office, Espoo, Finland, February 19, 2010 letter	101
Oracle Corporation, Jason M. Mahler, Vice President, Government Affairs, Washington, DC, February 19, 2010 letter	103
Paoletta, Mark R., Partner, Dickstein Shapiro, LLP, on behalf of McAfee, Inc., Washington, DC, February 19, 2010 letter	105
RIM, Robert E. Crow, Vice President, Industry, Government & University Relations, Washington, DC, February 19, 2010 letter	109
SAP, February 19, 2010 letter	111
Siemens, Kathleen Ambrose, Senior Vice President, Government Affairs, Washington, DC, letter	113
Skype, Josh Silverman, CEO Luxembourg, February 18, 2010 letter	114
Sprint, Vonya B. McCann, Senior Vice President Government Affairs, Washington DC, February 19, 2010 letter	119
Twitter, Alexander Macgillivray, General Counsel, San Francisco, California, February 19, 2010 letter	121
Verizon, Kathryn C. Brown, Senior Vice President, Public Policy Development & Corporate Responsibility, Washington, DC, February 19, 2010 letter	124
Vodafone, Vittorio Colao, Group Chief Executive, Berkshire, England, February 19, 2010 letter	127
Websense, Gene Hodges, Chief Executive Officer, San Diego, California, February 17, 2010 letter	128
Symantec, Enrique Salem, Mountain View, California, March 5, 2010 letter	131
Response from Tech Companies letters:	
3Com Corporation, Neal Goldman, Executive Vice President, Chief Administrative and Legal Officer, Marlborough, Massachusetts, August 12, 2009	133
3Com Corporation, Robert Mao, Chief Executive Officer, Marlborough, Massachusetts, March 22, 2010	135
Apple, Daniel Cooperman, Senior Vice President, General Counsel & Secretary, Cupertino, California, August 27, 2009 letter	136
AT&T Services, Inc., Timothy P. McKone, Executive Vice President, Federal Relations, Washington, DC, August 25, 2009 letter	145
CISCO Systems, Inc., Mark Chandler, Senior Vice President and General Counsel, San Jose, California, August 27, 2009 letter	148
Dell Inc., Gilbert F. Casellas, Vice President, Corporate Responsibility, Washington, DC, August 27, 2009 letter	151
eBay Inc., John Donahoe, President and Chief Executive Officer, San Jose, California, September 1, 2009 letter	154
Facebook, Timothy Sparapani, Director, Public Policy, Palo Alto, California, August 27, 2009 letter	155
Fortinet, John Whittle, Vice President, General Counsel, Sunnyvale, California, August 27, 2009 letter	160
Hewlett-Packard Company, Bruce Ives, Vice President and Deputy General Counsel, Global Alliances & Government Affairs, Palo Alto, California, August 27, 2009 letter	161
Lenovo, Elizabeth A. Hyman, Government Affairs, Washington, DC, August 14, 2009 letter	166
Motorola, Inc., Gregory Q. Brown, President & Chief Executive Officer, Schaumburg, Illinois, August 21, 2009 letter	167
MySpace.com, Rupert Murdoch, Chairman and Chief Executive Officer, New York, New York, August 24, 2010 letter	168
Nokia, Olli-Pekka Kallasvuori, President and Chief Executive Officer, Helsinki, Finland, August 27, 2009	170

	Page
Durbin, Hon. Richard J., a U.S. Senator from the State of Illinois and Hon. Tom Coburn, a U.S. Senator from the State of Oklahoma, joint letters to Tech Companies—Continued	
Nokia Siemens Networks, Rajeev Suri, Chief Executive Office, Espoo, Finland, August 27, 2009 letter	176
Paoletta, Mark R., Partner, Dickstein Shapiro, LLP, on behalf of McAfee, Inc., Washington, DC, August 27, 2009 letter	180
Siemens, Peter Loescher, President and Chief Executive Officer, Washington, DC, September 2, 2009 letters	185
Skype, Josh Silverman, CEO Luxembourg, August 26, 2009 letter	187
Sprint, Vonya B. McCann, Senior Vice President Government Affairs, Washington DC, August 27, 2009 letter	194
Symantec, Enrique Salem, Mountain View, California, January 20, 2010 letter	196
Verizon, Kathryn C. Brown, Senior Vice President, Public Policy Development & Corporate Responsibility, Washington, DC, August 27, 2009 letter	198
Vodafone, Vittorio Colao, Group Chief Executive, Berkshire, England, August 27, 2009 letter	200
Websense, Gene Hodges, Chief Executive Officer, San Diego, California, letter	201
Business for Social Responsibility (BSR), Washington, DC, statement	203
Black, Edward J., President & Chief Executive Officer, Computer & Communications Industry Association, Washington, DC, statement	206
Center for Democracy & Technology (CDT), Leslie Harris, President & Chief Executive Officer, Washington, DC, statement	208
Committee to Protect Journalists, New York, New York, statement	216
Ganesan, Arvind, Director, Business and Human Rights Program, Human Rights Watch, New York, New York, statement	219
Global Network Initiative, March 2, 2010 statement	224
Google, Nicole Wong, Deputy General Counsel, Washington, DC, statement and letter	232
Human Rights First, Washington, DC, statement	238
Internews Network, Washington, DC, statement	244
MacKinnon, Rebecca, Visiting Fellow at the Center for Information Technology Policy, Princeton University, Princeton, New Jersey, and Co-Founder, Global Voices Online, statement	247
Memarian, Omid, Iranian Blogger, San Francisco, California, statement	259
Microsoft, Pamela S. Passman, Corporate Vice President, Global Corporate Affairs, Redmond, Washington, letter and attachment	264
Posner, Michael H., Assistant Secretary for Democracy, Human Rights, and Labor, Department of State, Washington, DC, statement	270
Reporters Without Borders, Washington, DC, statement	274
Verma, Richard R., Assistant Secretary, Legislative Affairs, Department of State, Washington, DC, report	279
Washington Post, Caylan Ford, January 20, 2010, article	281
Weitzner, Daniel J., Associate Administrator for the Office of Policy Analysis and Development, National Telecommunications and Information Administration, Department of Commerce, Washington, DC, statement	283
Wong, Nicole, Vice President and Deputy General Counsel, Google Inc., Mountain View, California, statement	291
World Organization for Human Rights USA, Morton Sklar, Founding Executive Director Emeritus (retired), Washington, DC, statement	298
Yahoo, Jerry Yang, Chief Executive Officer, Sunnyvale, California, statement and attachment	306

GLOBAL INTERNET FREEDOM AND THE RULE OF LAW, PART II

TUESDAY, MARCH 2, 2010

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

The Subcommittee met, pursuant to notice, at 10:03 a.m., in room SD-226, Dirksen Senate Office Building, Hon. Richard J. Durbin, Chairman of the Subcommittee, presiding.

Present: Senators Durbin, Kaufman, Franken, and Coburn.

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

Chairman DURBIN. This hearing of the Judiciary Committee's Subcommittee on Human Rights and the Law will come to order. Today's hearing is "Global Internet Freedom and the Rule of Law, Part II."

After a few opening remarks, I will recognize those Senators who are in attendance for an opening statement and then go to our witnesses, whose attendance we appreciate.

This Subcommittee held our first hearing on this issue in May of 2008. At that hearing, we learned that repressive governments around the world censor the Internet and persecute human rights and democracy advocates who express their views online. Since then, the scale and scope of Internet censorship has increased dramatically.

At our hearing 2 years ago, I showed some pictures of censored Internet searches on Google and Yahoo!. Today I am going to demonstrate that, unfortunately, this censorship continues.

Let me start, if I can do this. What you are looking at here on the screen to your left is a Google.com search for the word "Tiananmen." You will find pictures of the famous Tiananmen Square protests in 1989, especially the iconic photo of a demonstrator standing in front of several tanks.

Now what you see is Google.cn, Google's China search engine, and a search for the same word, "Tiananmen." Here you will only find beautiful postcard images of Tiananmen Square.

Let me be clear. I am not singling out Google. Yahoo!, and Bing, Microsoft's search engine, also censor the Internet in China. And Baidu, the leading Chinese search engine, censors even more content than these American companies.

I want to commend Google again for announcing that they plan to stop censoring their Chinese search engine. I look forward to an update today on their efforts.

At our first hearing, we discussed the Global Network Initiative, or GNI, which was then being negotiated. The GNI is a voluntary code of conduct that requires technology companies to take reasonable measures to protect human rights.

Following the hearing, Senator Tom Coburn, this Subcommittee's Ranking Member, and I encouraged Google, Microsoft, and Yahoo! to complete the GNI negotiations, and the code was launched in October of 2008. I want to commend these three companies for their extraordinary leadership in promoting Internet freedom.

Since then, I have asked several dozen other companies to consider joining the GNI. Without objection, the companies' written responses will be entered into the hearing record and also will be made available on my website.

I am disappointed that a year and a half after the GNI started, no new companies have joined.

Based on the responses that I have received, only three companies—AT&T, McAfee, and Skype—have even committed to participating in a dialog about joining the GNI. One company, Websense, has indicated that they will join the GNI if the membership fee is waived.

Many companies told me that the GNI is not relevant to their company's business. The last 2 years have demonstrated that that is simply not true.

The explosive growth of social networking services, like Twitter and Facebook, has helped human rights activists organize and publicize human rights violations in Iran and other places around the world. However, repressive governments can use these same tools to monitor and crack down on advocates.

I invited Facebook and Twitter to testify today but they refused to appear.

Last year, the Chinese Government announced that they would require all computers sold in China to include software called "Green Dam," which censors political content and records user activity.

Thanks to the opposition from the U.S. Government and companies, the Chinese Government eventually backed down. This incident highlighted the human rights challenges faced by computer manufacturers.

I invited Hewlett-Packard and Apple to testify about these challenges today, and they also refused.

Filtering software produced by American companies has allegedly been used to censor the Internet in several countries with repressive governments.

I invited McAfee, which produces filtering software, to testify today. McAfee initially agreed but on Friday informed us that they were pulling out.

The bottom line is this: With a few notable exceptions, the technology industry seems unwilling to regulate itself and unwilling even to engage in a dialog with Congress about the serious human rights challenges that the industry faces.

In the face of this resistance, I have decided that it is time to take a more active position. At our hearing 2 years ago, I indicated that Congress could step in if the industry failed to take concrete action to protect Internet freedom.

Today I am announcing that I will introduce legislation that would require Internet companies to take reasonable steps to protect human rights or face civil or criminal liability. I look forward to working with my Republican colleague Senator Coburn and my other colleagues to enact this legislation into law.

I recognize that the technology industry faces difficult challenges when dealing with repressive governments, but we have a responsibility in the United States—and Congress shares in that responsibility—to ensure that American companies are not complicit in violating freedom of expression, a fundamental human right enshrined in the First Amendment of our Constitution and the Universal Declaration of Human Rights.

Now I want to recognize my colleague Senator Coburn, the Ranking Member of the Subcommittee.

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

Senator COBURN. Thank you, Mr. Chairman, and due to being a little bit under the weather, I think I will just ask that my opening statement be made a part of the record.

Chairman DURBIN. Without objection.

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

Chairman DURBIN. Senator Franken, do you have any opening remarks?

Senator FRANKEN. I do not. I look forward to the hearing, though, and thank you for calling it, Mr. Chairman.

Chairman DURBIN. Thanks, Senator Franken.

We are going to turn to our first panel of witnesses. The U.S. Government has an important role to play in promoting global Internet freedom and ensuring U.S. technology companies do not facilitate government repression. I look forward to hearing about the administration's plans to advance freedom of expression around the world. Our witnesses will each be given 5 minutes for an opening statement. Their complete written statements will be made part of the record and posted online.

I will ask now if the witnesses would please stand and raise their right hands to be sworn. 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?

Mr. POSNER. I do.

Mr. WEITZNER. I do.

Chairman DURBIN. Thank you. Let the record reflect that both of the witnesses answered in the affirmative.

Our first witness, Michael Posner, is the Assistant Secretary of State for Democracy, Human Rights, and Labor, our Government's top human rights official. Mr. Posner was previously founding Executive Director and President of Human Rights First, which he headed for 30 years. He has substantial expertise in corporate social responsibility and played a key role in founding the Global

Network Initiative. Mr. Posner has a bachelor's degree from the University of Michigan and a law degree from the University of California at Berkeley. He first testified before the Subcommittee last year when we held a hearing on the implementation of human rights treaties, and we are glad he is with us again.

Our following witness is Daniel Weitzner, the Associate Administrator for the Office of Policy Analysis and Development in the Commerce Department's National Telecommunications and Information Administration, and I think he is going to win a prize for the longest title of a witness appearing before our Committee. Mr. Weitzner is one of our Nation's leading experts on Internet policy. Prior to joining NTIA, Mr. Weitzner was Director of the MIT Computer Science and Artificial Intelligence Laboratory's Decentralized Information Group and Policy Director of the World Wide Web Consortium Technology and Society Activities. Mr. Weitzner was also co-founder and Deputy Director of the Center for Democracy and Technology, and Deputy Policy Director of the Electronic Frontier Foundation.

Your résumé is loaded with titles. That is terrific.

Mr. Weitzner has a bachelor's degree from Swarthmore and a law degree from Buffalo Law School. We thank you as well for joining us.

Mr. Posner, would you like to make your opening statement?

STATEMENT OF MICHAEL H. POSNER, ASSISTANT SECRETARY FOR DEMOCRACY, HUMAN RIGHTS, AND LABOR, U.S. DEPARTMENT OF STATE, WASHINGTON, D.C.

Mr. POSNER. Thank you. I want to thank you, Senator Durbin and Senator Coburn, for inviting me to testify and for your long-standing interest in this subject. I have followed this issue quite closely and the Subcommittee's involvement since your Part I hearing in 2008, and it is great that you are pursuing this.

When you first addressed Internet freedom, the primary concerns of those testifying were content filtering on the Internet and harassment and arrest of digital activists. These problems persist today. As Secretary Clinton highlighted in her January 21st speech on Internet freedom, the State Department continues to protest the arrest, detention, and harassment of bloggers in Iran, in China, in Egypt, in Vietnam, and elsewhere. And countries that seek to filter access to information are only becoming more skilled at doing so. These problems persist.

But the threats to Internet freedom are expanding beyond restricting access to content. As, again, Secretary Clinton described, repressive regimes are co-opting new media tools to crush dissent and deny human rights. And while the rapid increase in the use of mobile phones creates new platforms for connecting people and providing access to information, it also creates new threats to free expression and the free flow of information. So we have a major set of challenges.

The State Department since 2006 has had an Internet Freedom Task Force which has been re-launched as the Net Freedom Task Force, chaired by two of our Under Secretaries, and it is going to oversee the State Department's efforts on these issues. I want to just quickly cite three aspects of what we are doing.

The first is advancing Internet freedom through programming. Our effort is to provide unfettered safe access to information and communication. Beginning in 2008, the Bureau of Democracy, Human Rights, and Labor, which I lead, has implemented \$15 million in programming to support Internet freedom. I spell out some of the details in my testimony. We are also working with AID, with the Middle East Partnership Initiative on a range of specific initiatives aimed at providing training to journalists, civil society activists, political parties on the use of these new technologies.

The second thing that we are doing more broadly is monitoring and analyzing. Next week we will release the annual Human Rights Report of the State Department on human rights practices, annual Country Reports. One of the things we are going to do in the coming year is to review the reporting process and improve and expand on Internet freedom reporting, which is an essential piece of what we need to be doing. We are going to make the reports more accessible to people around the world who have limited access to the Internet, and we are going to increase the capacity of our embassy officers to monitor and respond when there are threats to Internet freedom.

And that is really the third aspect of what we are doing—responding. It is, unfortunately, too often the case that those who are involved in human rights and other advocacy are themselves targeted because of their advocacy, and those who are using the Internet and social networking sites are being attacked precisely because they are communicating effectively.

For example, last fall, when a popular social networking site was blocked in Vietnam, we raised the issues with officials in Hanoi and in Washington. When bloggers in countries such as China and Vietnam and Egypt and Iran are threatened, we speak out publicly on their behalf. This is an important part of what we can be and need to be doing.

I want to just say a last comment, and it relates to what you spoke about, Senator Durbin, in your opening. This is an issue where the Government has a role, but the private sector also has a role. As you noted, I was involved before coming into Government in the creation of the Global Network initiative, which is a multi-stakeholder initiative that brings together companies, NGO's, academic experts, and social and investing firms.

I think it is really critical that we and you work to figure out ways for companies to step up and take responsibility here. We cannot do it alone, and companies acting alone cannot make a difference. There needs to be a collective response, and I am personally very committed, as are others in the State Department, to trying to find ways to work collectively with the private sector to make a difference in this area.

Thank you very much.

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

Chairman DURBIN. Mr. Weitzner.

STATEMENT OF DANIEL J. WEITZNER, ASSOCIATE ADMINISTRATOR FOR THE OFFICE OF POLICY ANALYSIS AND DEVELOPMENT, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE, WASHINGTON, D.C.

Mr. WEITZNER. Chairman Durbin and Ranking Member Coburn, members of the Subcommittee, thank you for this invitation to testify on behalf of the Department of Commerce and the National Telecommunications and Information Administration—I will work on shortening titles—on the global challenges facing the Internet industry. As an advocate of economic growth, innovation, and exports, the Department of Commerce's goal is to support a global, open Internet as a platform for the free flow of information, goods, and services. The Department of Commerce is committed to our role as partner with U.S. companies, large and small, as they grapple with the challenges of operating in countries that reject openness, transparency, and the free flow of information.

The great innovative energy of the Internet is due to the fact that even the smallest U.S. Internet startups can be reached by user all over the world. With this strength, we must also recognize that U.S. companies can become the target of arbitrary foreign laws, even if they have no offices in that country.

Today I will summarize the challenges we see facing U.S. companies, discuss the importance of transparency on the Internet, and update you on the Commerce Department's activities to support a commercial, robust, and transparent Internet. Let me just highlight three major threats that we see very briefly.

First, U.S. companies are often pressured to block or filter Internet content or communications absent any evidence of illegality, based on rules that are unclear, unwritten, and often lacking due process or transparency.

Second, some governments would require their Internet service providers to assist in electronic surveillance without due process or adequate judicial supervision. This puts these companies in untenable situations that they should not have to face.

U.S. companies, third, risk being the victims of hacking attempts sponsored by overseas criminals, foreign governments, or loose-knit groups of both working together. In this era of globally integrated, cloud computing platforms, security threats in one country can put the entire global enterprise at risk. Worse, security has become a pretext often for forced compliance with government-imposed technically deficient standards, disadvantaging U.S. companies which support global Internet standards, and putting the entire Internet at risk.

Unfair treatment of Internet users and providers threatens the Internet's fundamental modus operandi—transparency. Open technical standards have enabled rapid innovation and global interoperability of the Internet and the applications that run on it.

Despite recent attention to vulnerabilities in the Internet infrastructure, we must not lose sight of the extraordinary engineering achievements that enable global citizens to communicate through a common platform. Transparency is at the heart of the Internet's success.

Looking forward, the Commerce Department will continue its successful tradition of working with stakeholders to develop Government, industry, civil society partnerships supporting Internet development. We have been heartened by the Global Network Initiative's ongoing efforts to develop a voluntary code of conduct for Internet companies. The Government must be a full partner in this effort, we believe, standing up for individuals and businesses when the free flow of information and human rights are threatened.

Ensuring that the Internet is open for innovation and social progress is a vital priority for the Department. In the early months of the new administration, we assembled a cross-department Internet Policy Task Force whose mission is to identify leading public policy and operational challenges in the Internet environment. Our task force leverages expertise across many bureaus, including international communications policy, trade, intellectual property protection, business advocacy, and corporate responsibility. Our work began with developing a new Internet privacy and cybersecurity. The task force has convened consultations with major U.S. corporations and innovators across academia and civil society. We have now added consideration of global trade barriers along with online copyright enforcement and Internet governance.

In the coming months, outreach will continue as the task force will issue Notices of Inquiry on these topics. Based on this feedback, the task force will focus departmental resources on this challenge and contribute to an administration-wide public policy development.

In closing, let me say from my own experience that the Internet was created and has grown to global scale because of a unique combination of cooperation and transparency. Academic and commercial researchers, as you know, came together to create and extend the underlying Internet technology. As the Internet grew, it was often cooperative efforts of industry, civil society, and Government that came together to solve hard social and legal problems.

The threats to the free flow of information on the Internet are serious. We should look to solve them as much as possible with the unique cooperative, transparent spirit that gave us the Internet in the first place.

I thank you again for the opportunity to be here and for your longstanding attention to this important issue, and I look forward to your questions.

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

Chairman DURBIN. Thanks a lot.

We asked Facebook to testify, and they said, "We have no business operations in China or, for that matter, in most of the countries of the world." They went on to say, "As a young startup, our resources and influence are limited. We do not have the resources to devote to GNI membership."

But here are the facts. Facebook has over 400 million users, which makes it the second most viewed website in the world. About 70 percent of Facebook users are outside the United States. Facebook has over 1,000 employees, hundreds of millions of dollars in annual revenues, and is worth billions of dollars. That is hardly a mom-and-pop operation that cannot afford to be a part of GNI.

And Facebook acknowledges that it engages in censorship. In their letter to me, Facebook said, and I quote, “When content shared from a particular jurisdiction violates that jurisdiction’s local laws or customs, Facebook may take down that content.”

Mr. Posner, it is my understanding that Facebook recently asked the State Department for help when they were blocked in Vietnam, and you responded by raising the issue with the Vietnamese Government. Is that right?

Mr. POSNER. Yes, we have responded—a number of companies have come to us. Facebook is one of them. And we are obviously trying to promote Internet freedom, so we are trying to be cooperative with all of them.

Chairman DURBIN. So if Facebook expects our Government to help in resolving efforts to censor their service, it only seems reasonable that they accept some responsibility themselves for addressing human rights issues.

Mr. Posner, does Facebook face human rights challenges such as censorship that GNI would address?

Mr. POSNER. You know, again, I do not want to single out one particular company, but I think it is fair to say that companies like Facebook and Twitter are certainly susceptible to a lot of the pressures that we have seen others face. The technology is changing. The world is changing. Governments are getting much more aggressive in trying to regulate and control content. So I think it is——

Chairman DURBIN. I do not want to single out one company either, so let me single out another one. Let us take Twitter.

[Laughter.]

Chairman DURBIN. In a letter to me, Twitter expressed confidence they were having a positive impact on human rights, and I believe that. They said, and I quote, “Twitter is a triumph of humanity, not technology.” Twitter has helped activists to organize and publicize human rights violations, but they also face human rights challenges. For example, there are reports the Iranian Government is tracking down opposition activists who use Twitter. However, in their letter to me, Twitter declined to join the GNI saying, and I quote, “It is our initial sense that GNI’s draft policies, processes, and fees are better suited to bigger companies who have actual operations in sensitive regions.”

Mr. Posner, does Twitter face human rights challenges that the GNI could address?

Mr. POSNER. Yes, they do, and I think one of the things that makes the GNI to me an important part of the solution here is that companies are going to learn from each other. There is not one company that is going to have a monopoly on creativity or thoughts about how to deal with this. They need to work collectively, and that is part of what this initiative is designed to do.

Chairman DURBIN. In our next panel, Omid Memarian, an Iranian blogger who is a witness today, says in his testimony, and I quote, “It was not the Iranian Government who shut down my website, it was the domain and host provider in the United States that did it.”

Testimony by Rebecca MacKinnon, another witness on our second panel, indicates that U.S. web hosting companies have also denied services to political opposition groups in Zimbabwe and Syria.

I would like to ask you both: What can be done to ensure that U.S. sanctions and exports controls do not prevent U.S. companies from providing Internet technology and services like website hosting to human rights and democracy activists living under repressive governments?

Mr. WEITZNER. As you know, Mr. Chairman, the jurisdiction for export controls is shared between the Commerce Department. We enforce our Export Administration regulations and other rules of the State Department as well as the Treasury Department.

As to services such as Twitter and others that you mentioned that do not employ any encryption software on the user end, as far as we understand, those services are freely available around the world from the perspective of U.S. regulations. Obviously, as you note, other countries may block access to those services. But the Commerce Department's Export Administration regulations do not prevent anyone in the world from using a service like Twitter. That is because it is a service that is based on the Web; it does not require the installation of software.

It is also the case that under Commerce Department regulations publicly available, downloadable software with encryption can be used widely.

Chairman DURBIN. Let me ask about another issue that is related. Some commentators have expressed concern about the appearance that the State Department is too close to some American Internet companies. For example, last week, Twitter CEO Jack Dorsey was a member of an official State Department delegation to Russia. Top State Department officials used Twitter to post details about their personal lives. Technology expert Evgeny Morozov said, and I quote, "The kind of message that it sends to the rest of the world—that Google, Facebook, and Twitter are now just extensions of the U.S. State Department—may simply endanger the lives of those who use such services in authoritarian countries. It is hardly surprising that the Iranian Government has begun to view all Twitter users with the utmost suspicion."

Mr. Posner, are you concerned about the perception that the State Department is too close to companies like Twitter and Facebook? And how can we combat the impression that these companies are just an arm of our Government?

Mr. POSNER. I think we have to be able to work in multiple ways as a Government. The fact that there are these social networking sites or Internet sites that deploy or allow information to be disseminated quickly means that they are a tool for all governments and for private citizens. We should not reject that. But at the same time, I think we have to be clear that there is a separation between Government and these private companies. They are not part of the Government. And there are certain obligations we are to hold their feet to the fire to be acting responsibly as companies.

So I think we need to be really operating in multiple tracks here, not to deny ourselves the ability to use the excellent tools that they provide, but at the same time keeping the lines clear of who we are

and who the companies are and holding them accountable for their own actions.

Chairman DURBIN. Thank you.

Senator Coburn.

Senator COBURN. Thank you.

Mr. Posner, you talked about the three things that you all are doing in terms of programming, monitoring, and analyzing, then responding, and you spoke specifically about responding to two or three different instances. Vietnam I think was one that you mentioned.

What has been the effect of that response?

Mr. POSNER. This is a long-term and tough subject for us to claim immediate results. It is not going to happen that way. Governments are testing the limits, and we're pushing back.

I think in the long run we are going to succeed because I think efforts by governments to control people's ideas are not going to succeed. People are going to find creative ways to circumvent whatever restrictions governments put up.

But I think we just have to be resolute in saying we are absolutely dedicated, as Secretary Clinton said, to a free, open Internet and communications environment without restrictions, and we are going to keep pushing for that. And when governments push back, we are going to be there to say this is counter to American values and American foreign policy.

Senator COBURN. So there is definitely going to be a consistency to your message and a constance to your message.

Mr. POSNER. If we are not consistent, we are not going to succeed. Yes.

Senator COBURN. OK. Mr. Weitzner, you mentioned the GNI in your testimony. Given your unique perspective of the diversity of all the companies that make up the industry, that offer Internet-based goods and services around the world, do you see GNI as a framework that will fit every one of those companies? Or is there the case that maybe this does not fit some of them?

Mr. WEITZNER. From the perspective of the efforts that we imagine at the Commerce Department, our main interest is to be a partner with the GNI. It seems unlikely that every single Internet company in the United States would join. We certainly hope more do. These organizations have to figure out how to create the proper kind of fit between their mission and those whom they hope to serve. That is not an easy challenge, as you know, but we think it is important.

From the Commerce Department's perspective, we hear from companies large and small and across a number of sectors of the Internet economy. Certainly small startups may not be able to fully participate in the GNI, but we think, first of all, they will benefit from the efforts of an organization like that, and we are looking very carefully at how we can make the trade assistance resources we have available on the ground in over 60 countries around the world available to those U.S. companies who, for whatever reason, do not fit as well.

Senator COBURN. But you do feel that ultimately they all will have some benefit, directly or indirectly.

Mr. WEITZNER. I think that if the GNI can succeed at its efforts to bring greater transparency and a set of commonly accepted best practices, that would benefit the Internet as a whole.

Senator COBURN. What kind of guidance does your Department give to U.S. companies offering Internet-based goods and services in Internet-restricted countries to overcome the challenges that you outlined in your testimony?

Mr. WEITZNER. I would not say there is a single answer to that question, but as I noted, the Commerce Department resources, working along with State Department resources in many countries, works on a case-by-case basis to work through barriers or misunderstandings that companies face. When those barriers are seen to be too hard to resolve in individual cases, we can escalate those to discussions with the governments, and often a government-to-government discussion at whatever level can be helpful in a way that the company may not be able to muster all by itself.

This is especially true for smaller companies, for companies that do not have the international profile of some of the cases that we have seen in the news. So, again, we think that we will have an essential role to play in helping U.S. companies that way.

Senator COBURN. Are there some instances of success where you have been able to accomplish that?

Mr. WEITZNER. Well, very often these are efforts that require co-operation across the executive branch. I would point to the recent interactions involving the Green Dam Internet filtering requirement that was proposed by the Chinese Government. As that issue was raised to various parts of the U.S. Government, including the Commerce Department, the International Trade Administration, the USTR, State Department, and others, we were able to have a dialog with the Chinese Government that we think produced results.

Senator COBURN. OK. The Department of Commerce seems to be on the forefront of some of the issues we are discussing today. But, on the other hand, I was startled to hear that efforts to target Internet policy changes seem to have only just begun.

Is the Interagency Internet Policy Task Force the first such initiative undertaken by the Department?

Mr. WEITZNER. The Department of Commerce's efforts in Internet policy go back to more or less the beginning of the commercial Internet in the mid-1990's, so early work was done in the Department of Commerce in laying out a framework for global electronic commerce and laying privacy rules and approaches that would be appropriate for the Internet. So I am proud to say there is a long-standing tradition at the Commerce Department far pre-dating our work, and we intend to continue that.

Senator COBURN. How long before a Notice of Inquiry runs in the Federal Register to solicit additional outside opinions?

Mr. WEITZNER. We are hoping to do this in the next couple of months.

Senator COBURN. Why can't it be done immediately?

Mr. WEITZNER. Well, we have been engaging in discussions with a variety of companies and technical experts and academics to make sure we understand the questions we ought to be asking. So

we are actively engaged in that, and we are going to get it out just as soon as we can.

Senator COBURN. That is fair. When does the task force anticipate making formal recommendations to the Secretary of Commerce?

Mr. WEITZNER. We will be working over the course of this year, and we expect by the end of the year we will have recommendations. But we will be contributing based on what we learned in an informal way both to Commerce Department efforts and to administration-wide efforts. So we view this as an ongoing effort.

Senator COBURN. You have this tremendous knowledge and tremendous experience. Is it always going to be possible for U.S. companies to operate in ways that support a global open Internet that facilitates the free flow of information, goods, and services even with countries that do not share those values? And how do we get there?

Mr. WEITZNER. I hesitate to say anything is always possible. I think that it will be possible, and I share my colleague Secretary Posner's optimism that we will be able to make progress on this. I think the history of the Internet has been the spread of a recognition that openness is good for everyone.

Senator COBURN. It is a powerful tool.

Mr. WEITZNER. Yes.

Senator COBURN. OK. Thank you, Mr. Chairman.

Chairman DURBIN. Senator Franken.

Senator FRANKEN. Thank you, Mr. Chairman.

Mr. Posner, Congress has reserved tens of millions of dollars for funding anti-censorship initiatives. Just last December, your Bureau called for \$5 million of this funding. However, as a bipartisan group of Senators has pointed out, the application required a significant "in-country presence," requiring the groups developing anti-censorship software, for example, to actually physically be present in an authoritarian country.

I am no IT expert, but the impression I get is that software is pretty portable. I also get the impression that it is hard to live in an authoritarian country as an anti-censorship programmer in a country like Iran.

Why do we have this requirement? And is it necessary?

Mr. POSNER. Senator, I think there has been some misunderstanding of that requirement, and I will say we have gotten a range of very exciting proposals from more than 20 different entities.

What we are trying to do is create opportunities for people operating in tough, repressive places like Iran to get access to information. When we talk about presence, we are not talking about having servers on the scene or complicated technical equipment. What we are trying to do is find entities, a range of different groups, who are looking, as we are, creatively at how to use Internet, how to use telephone applications to better communicate within their own societies. So the field is wide open, and we have a range of different applicants for that money, many of whom are not physically located in the countries that are—

Senator FRANKEN. In the proposal it says the bulk of project activities must take place in-country and last between 1 and 3 years.

Mr. POSNER. Yes, but when we say that, what we are talking about is—for example, let us take the example of Iran. What we are interested in doing is providing the kind of training, assistance, protection to people, Iranians, who are in within their own society trying to open up the free flow of information and access to information. We are working with a range of groups that are not themselves based in Iran or in China or in any of these countries, but we are trying to create opportunities for people inside their own countries, their own societies, to communicate more effectively. That is the purpose of that language.

Senator FRANKEN. OK. I am not sure I totally follow it, but let us go somewhere else. The Washington Post specifically criticized the State Department for not giving a cent to a group called the Global Internet Freedom Consortium, and, Mr. Chairman, without objection, I would like to add a copy of that editorial for the record.

Chairman DURBIN. Without objection.

[The editorial appears as a submission for the record.]

Senator FRANKEN. According to the Wall Street Journal, these are the guys who developed the software that allowed protesters in Iran to communicate during and after the government crackdown. Can you speak to the Post editorial? Why hasn't this group received any funding?

Mr. POSNER. First of all, the group you mention is one of the 20-some that applied for funding in December, and those applications or that money is now being disbursed—or we are reviewing all of the applications and will make a decision in the next few months. And the competition was open, and we encouraged them to apply and they did, which is a good sign.

Our approach has been that there is not one magic answer to how to circumvent these restrictions, that there needs to be a range of tools, a range of different approaches. We sort of view ourselves as somewhat like the venture capital firms in the Silicon Valley trying a lot of different things. The technology—

Senator FRANKEN. But this group seemed particularly successful and is not one that received funding.

Mr. POSNER. There are different views about how successful any one of these has been, and we are looking at that. But, you know, we are absolutely open to their being a candidate for funding and are looking at it very seriously.

Senator FRANKEN. Thank you.

Mr. Weitzner, I know that free trade agreements or trade agreements are negotiated by the United States Trade Representative, not your Department, but I still want to ask you this question. Over time, our free trade agreements have come to include robust protections for workers and for the environment. One of our latest FTAs, the Korean FTA, includes a provision protecting “the free flow of information in facilitating trade,” but it only covers international information flows, not intra-country censorship, and also isn't mandatory.

Will this administration support a simple mandatory ban on political censorship on the Internet in future trade agreements?

Mr. WEITZNER. That is a question I am not prepared to speak to right here, but will certainly take it back and consider it. I think that as we look at the free trade agreements that we have that

would be amended and the new ones that are being negotiated, it is certainly appropriate to consider the range of issues that affect the open Internet. It is clearly in the interest of promoting free trade to have an open Internet, and we will be happy to come back with you and talk in more detail about your suggestion.

Senator FRANKEN. OK. And you mentioned that part of your portfolio is trade and intellectual property, so I just wanted to ask—we are talking about a free flow of information and Internet freedom here, but I want to also talk for a second, that as long as we are considering putting this kind of restrictions in our trade agreements that will restrict censorship, what are we doing on intellectual property? And can we put these together to prevent countries like China from ripping off our intellectual property, our movies, music, et cetera?

Mr. WEITZNER. As you probably know, Senator, a number of the free trade agreements that we have already negotiated have intellectual property protection provisions in them, and there are negotiations ongoing in other venues to advance that to other countries as well. So it is an agenda that is being actively pursued by this administration.

Senator FRANKEN. Thank you.

Thank you, Mr. Chairman.

Chairman DURBIN. Senator Kaufman.

Senator KAUFMAN. Mr. Chairman, I want to thank you for holding this hearing. I think it is very timely, it is important. There is hardly anything I can think of that is more important than the free exchange of ideas if we are going to be successful in having a peaceful world over the next 20, 30, 40, 50 years.

I spent 13 years on the Broadcasting Board of Governors, and we wrestled time and again with the problem of Internet freedom and how you deal with it in certain countries. And I would just like to reinforce what Mr. Posner said, and that is, in the late 1990s, we went out to Silicon Valley and talked to the experts out there about how do you do this battle and how can you win. And they all to a person reassured us that they cannot block what it is they were sending. It is always easier to send a message than it is to block. It is sort of like nuclear where they said one, two, three, four missiles, knocking them down is much more difficult than putting them up. So the key to this thing in the end is being creative and doing more, and people will find their way. That in no way, in no way, to know how difficult it is for people to deal—they are non-technical people—with these different techniques that are available.

The second thing, I would like to really follow up strongly on what Senator Coburn said. I am absolutely convinced that one of the secrets of this is government to government. These folks, if they think this is important—for instance, if we are dealing with a country that we all know—without naming any countries—there are always 20 things we want to talk about. If this is not on the agenda for discussion, they get the clear message we do not care about it. And far too often this issue has not been on the agenda, not just the Internet freedom but freedom of the press.

So I am just saying that in those discussions when you go overseas, if you do not raise this, they will get the message that this

really does not matter. So Senator Coburn is right on point in my opinion in saying that we have got to stress the government-to-government part.

Can both of you kind of comment on the recent conviction of Google executives in Italy for third-party content and what it means for Internet freedom and what we can do about it, both in the State Department and the Commerce Department?

Mr. POSNER. It is distressing, to say the least, that Italian authorities have sought to make representatives, local representatives of a private company in a sense the censors of content and, you know, we are clearly concerned about the ramifications of that as it would spread out across the globe. There are obviously sensitivities. The companies, I think, have got to take, again, responsibility for monitoring the content, but this is a company that, to my mind, was trying to do that and, when they were informed about the content, acted appropriately and yet they are being targeted by a government.

So I think this is actually a very important case and one that we need to respond to and follow very closely.

Mr. WEITZNER. Thank you, Senator. I would agree that their case is very important, and the larger issue that it raises is probably even more important.

One of the first steps that the United States took in legislating and creating a legal environment for the Internet was to recognize that if we place third parties in the position of—whether they are Internet service providers or those who host content, such as YouTube, if you place those parties in the position of having to figure out what the rules about third-party content might be, figure out whether they might be liable, the Internet really would grind to a halt. And I think that it is an issue that I think we tackled early on in the United States, and it is one that I hope we can raise awareness of around the world as we go forward.

Senator KAUFMAN. And I hope there, again, we will do government-to-government, multilateral—this could bring the entire Internet to a halt, and it is not in the interest of anyone to have this happen. And if Italy gets away with it, then more countries will do the same thing.

One of the models I think we should use going forward on this is not voluntary matters, the VOICE Act, to deal with Iran and the way Iran blocks the Internet and the things they do. And the VOICE Act has the government promoting ways to get around, to help folks get around the Iranian blocking of the Internet. And, Mr. Posner, we are expecting a report soon. Can you kind of give me the status of where we are on that?

Mr. POSNER. As I understand it, the report was—a draft of it has been prepared by the BBG, and it is now being reviewed in an interagency process, and I think you should get it shortly. But it is certainly underway, and I will make sure that you get it very soon.

Senator KAUFMAN. Good. Thank you.

Are there any examples beyond Google, what Google is doing in China, of corporations taking on charges for Internet freedom that you can think of off the top of your head, some good stories?

Mr. POSNER. Yes, I would say one of the things that, again, has been encouraging to me about the companies that have participated in the Global Network Initiative is that they have taken internally steps to do things to preempt or to anticipate problems. So, for example, we talk about Google. I would also talk about Yahoo! in the same breath. They have really internally undertaken to make human rights part of their internal decisionmaking process, and when they have gone into new markets, they have undertaken to review and do country analyses so they know what they are getting themselves into.

I think those sorts of steps, while they are not dramatic, are essential. If we are really talking companies stepping up and taking responsibility, it starts within their own corporate structure, and it starts with their understanding of the places where they are operating and taking the time to really evaluate the human rights and free expression risks. So I think that is the kind of initiative that I am looking at and hoping that other companies will follow.

Senator KAUFMAN. You know, I think that is a business decision, having worked in corporate America, that is a decision you make, whether you go into a country where clearly you are going to have a problem. But, you know, many people attribute the end of segregation in the South to when American corporations decided they were going to do away with the good neighbor policy. And I think, with all due respect—and I mean with all due respect—until corporations decide that they are not going to abide by the Internet freedom good neighbor policy, we are going to be aiding and abetting, as we have in the past, regimes from blocking the Internet, and a lot of it is being done with U.S. technology and U.S. companies.

So I am sensitive to the fact that internally we have to deal with it, but at some point someone has got to get up and say, “I am not going to do it.” And, you know, the slippery slopes we all travel, and we all know this, and that is, when you say, “If I don’t do it, someone else will,” that is the time to stop back and examine your conscience on what is going on.

The other thing that is kind of an interest of mine—and I will just finish with this, if that is OK—is U.S. companies. I mean, what is a U.S. company today with multinational corporations having so many interests around the world, how do you deal—do you deal with non-U.S. companies and what they are doing about Internet freedom?

Mr. POSNER. I think one of the challenges we face now and the GNI will face in its own operation is trying to re-engage particularly with some of the Western European governments and companies and some of the Asian companies, the Japanese and Koreans and others. This cannot just be a U.S.-based initiative. And in the early negotiations or discussions of the GNI, several of the telephone companies from Europe were nominally involved, preliminarily involved, and they pulled back. We are very keen to get European governments and European companies in particular, and some of these Asian companies as well, to get engaged as well. This has to be a collective response.

Senator KAUFMAN. Thank you.

Thank you, Mr. Chairman.

Chairman DURBIN. Thank you very much.

I would like to ask a question that may betray my legal training back in the early days of our Republic, but I am trying to put in my own mind a spectrum of activities where it would be—most of us would approve of an Internet company cooperating with the Government.

Example one, child pornography, and our Government in the course of an investigation asks for the identification of those who have had access to certain websites which we believe would be the basis for a criminal prosecution.

Example two, people venting their political feelings bordering on the suggestion of violence against certain public officials.

No. 3, specific threats of violence against an individual, a Member of Congress or the President of the United States.

No. 4, involvement in terrorism, working with groups that are literally trying to do us harm.

No. 5, the disclosure of information classified by our Government as top secret which may compromise our National security.

Going up the spectrum here, you can see the severity of the issue and the seriousness of the issue. And I am wondering—I do not want to oversimplify what we are doing here and say it should be easy for companies doing business in other countries to know where to draw the line. Where does GNI draw the line? How do they draw the line?

Mr. Posner.

Mr. POSNER. It is an excellent question, and, you know, it is probably one of the toughest questions to deal with in a practical way. That list you give, we have all sorts of constraints now in society against pornography and against promoting or supporting terrorism or engaging in violent acts or promoting that. I think we have to use the same frame globally and say there are certain activities that the Government has an obligation to prevent as a matter of law enforcement.

The challenge we face is that the concept of law enforcement and national security takes on a very different coloration if you are talking about the Government of Iran or the Government of China or any others. And the notion of national security becomes so overwhelmingly broad that what we would consider protected speech, political speech, you know, criticism of government action, comes under that rubric.

So that is the challenge. Companies say, and with some justification, we need to follow local law. Somebody tells us there is a violation of national security; we need to be responsive to that.

I think the hardest, almost the hardest question is when do you say, “No, that does not feel to us like a legitimate national security question; you just do not like being criticized”? And that is the world we live in.

Chairman DURBIN. How does GNI draw the line?

Mr. POSNER. Well, to be honest, we had many, many discussions in the negotiation of the GNI on exactly that question, and I think those are going to be the hardest calls for companies to make or for Government to make.

The good news for me is there is an awful lot of activity and work that can be done that is short of that where you are dealing

with pure speech and where, you know, your example, the video, you know, the Tiananmen Square image on Google.com ought to be the same one that is on the Google site that we all look at.

And so there is a lot of room to be done in promoting free expression that I think where there is clearly a path forward if companies work together, push the limits, and as Senator Kaufman said, we reinforce that with Government action.

Chairman DURBIN. Mr. Weitzner.

Mr. WEITZNER. Thank you. Let me try to address the procedural aspect of that question. I think the substantive nature of that spectrum that you drew out, we recognize as some national variations around the world, and we have always had to deal with that. I think some part of the way that we can come together in an environment where the Internet can actually function globally, where these national differences can be accounted for where they are reasonable, but where they do not become overall barriers to the free flow of information and to the viability of the Internet, is to keep in mind two important principles.

I think that we should have a basic expectation of due process. National rules may vary, but when they become arbitrary, I think we all have a concern, and that is obviously of most concern for the individual rights at stake.

By the same token, transparency and predictability of these rules, wherever they fall on that spectrum and however that spectrum evolves over time, are essential if we are going to have a viable commercial environment because, as we have discussed, companies simply cannot make these choices by just throwing darts at a board and trying to figure out what is in the mind of the governments that have real power over them.

I would say that if we can stick to those procedural motions of due process and transparency, we have some chance as an international community of evolving toward a set of norms that everyone can live with. We will never, I think, close the gap completely, sad to say, but what we have to work for, both for the sake of human rights and for the sake of U.S. innovation and global innovation on the Internet, is making sure that we have an environment in which everyone is able to function with some predictability and stability.

Chairman DURBIN. Thank you.

Senator COBURN. Senator Franken.

Senator FRANKEN. I guess I just wanted to make this one thing clearer for people listening or watching about the situation in Italy, because I think we talked on a pretty high level about it. Basically if you are a platform in America, you are not responsible for—you cannot be put in prison because somebody used your platform to print something that was libelous or something like that, and that allows for the free flow of information; whereas, in Italy what has happened is that Google executives have been prosecuted and convicted—right?—and will have to go to prison just because something showed up using their platform.

I am only saying this because—I just wanted to clarify it for people listening. Sometimes I think we operate on a higher level here than—or maybe I am mistaken. Maybe people listening are operating on a higher level than we are—

Mr. WEITZNER. Senator, hopefully there is some of both.

[Laughter.]

Mr. WEITZNER. I know you have a witness from Google on the next panel, so I do not want to speak for them. But, yes, I think it is a very stark situation. There were criminal convictions handed out, and indeed, this situation—and it is indeed the case that that sort of conviction would not have happened under United States law because of the protections that we provide to service providers and platform—

Senator FRANKEN. I want people to understand this. I remember when MoveOn had a contest to do ads, and it was basically anti-Bush ads. And one of the people sent in an ad comparing the Bush administration to the Nazi regime, which was just wrong. You do not do that. The Nazi regime was way, way, way beyond parallel. I mean, you cannot do that.

Now, MoveOn did not know it was up. When it was alerted that it was up, it took it down. But I kept hearing shows like on Fox saying MoveOn put on an ad comparing, you know, Bush with Hitler. You know, I just want people to understand what that was and what a platform is and that we cannot hold those platforms responsible for things that people put up on the platform.

That is all. Thank you.

Chairman DURBIN. Senator Kaufman.

Senator KAUFMAN. Yes, they cannot police that.

Mr. Chairman, I think I would ask you, in your comments on legally how we should deal with this, I think if you go to these other countries—and correct me if I am wrong—in my experience in them, all—not just the Internet—all jamming of broadcasts, all closing down, they do not say we are doing anything about it. This is not about the public discourse. This is about child pornography. That is the No. 1—I mean, so American corporations, when you go to them early on in this process and say, “What are you doing?” “Oh, no, we are just providing equipment to deal with child pornography.” When, in fact, when you go to the country and you see what is on the air, clearly they are blocking everything. This is like Potter Stewart’s—you know, you pornography, you know when you see it.

So legally they will say, “We are doing child pornography. We are controlling national security.” They usually say national security. They use that in these very sophisticated countries as why they are blocking the Internet. Is that a fair analysis of what is going on?

Mr. POSNER. It is. You know, in fact, after Secretary Clinton gave her speech in January, I talked to several Chinese activists, and that is exactly the way the Chinese Government and Chinese media were portraying the speech: “This is not about free speech. It is a pretext. They just want to promote pornography.”

So we sort of live in a world where we assume there is a rational discourse about these things. In fact, our intentions are being challenged all the time. And the notion of a kind of free, open Internet is assumed to be for purposes that we, in fact, would also not regard as legitimate.

Chairman DURBIN. Thank you, Senator Kaufman, and thanks to this first panel. We appreciate it. We may have some follow-up questions and hope you can answer them in a timely fashion.

If the second panel would please come to the table, I am going to ask for unanimous consent to enter into the record the assessment of fees for the GNI, which I believe will be referred to by one of the witnesses in the second panel. One of the companies that was asked whether it would participate in GNI said that if the fee would be waived, they would consider it. The fees range from \$2,000 annual fees for companies with annual revenues up to \$100 million to \$60,000 annual fees for companies with revenues over \$50 billion. It would seem that the fee should not be an impediment or obstacle to those that want to actively participate in what we consider to be a very valuable thing to the industry.

[The information referred to appears as a submission for the record.]

Chairman DURBIN. Let me start by asking the three witnesses who are before us to please stand and raise your right hand. 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.

Ms. MACKINNON. I do.

Mr. MEMARIAN. I do.

Chairman DURBIN. Thank you. Let the record reflect that the three witnesses answered in the affirmative.

The first witness is Nicole Wong. She is Vice President and Deputy General Counsel at Google, where she is primarily responsible for company products and regulatory matters.

Ms. Wong, again, I want to commend you and your company, Google, for engaging with Congress on this critical issue.

Prior to joining Google, Ms. Wong was a partner at the law firm of Perkins Cole. In 2006, she was named one of the Best Lawyers Under 40 by the National Asian Pacific American Bar Association. Ms. Wong holds a law degree and a master's degree in journalism from the University of California at Berkeley. She testified before this Subcommittee at our first hearing in 2008. We thank you for joining us again.

Following her, Rebecca MacKinnon, a Visiting Fellow at Princeton University's Center for Information Technology Policy, co-founded Global Voices Online, an international network of journalists and bloggers. She is a founding member of the Global Network Initiative. Ms. MacKinnon has been a research fellow at Harvard's Berkman Center for Internet and Society and assistant professor at the University of Hong Kong's Journalism and Media Studies Center. She previously worked as a journalist with CNN in Beijing for 9 years, serving as CNN's Beijing Bureau chief correspondent from 1998 to 2001. She holds a bachelor's degree from Harvard College. Thank you for being here.

And our final witness is Omid Memarian, a journalist and blogger. He was a Rotary Peace Fellow at the University of California at Berkeley Graduate School of Journalism. He received Human Rights Watch's highest honor in 2005, the Human Rights Defender Award. He was awarded the Golden Pen Award at the National Press Festival in Iran in 2002. He has been blogging in English and Persian since 2002. He has a bachelor's degree from Azad University.

Mr. Memarian, I know the Iranian Government persecuted you simply because you exercised your freedom of speech. Thank you for having the courage to continue to speak out and for joining us today.

Let us start with Ms. Wong. You have 5 minutes. Your written statement will be put in the record in its entirety. Please proceed.

**STATEMENT OF NICOLE WONG, VICE PRESIDENT AND DEPUTY
GENERAL COUNSEL, GOOGLE INC., MOUNTAIN VIEW, CALI-
FORNIA**

Ms. WONG. Thank you, Chairman Durbin, Ranking Member Coburn, and members of this Committee. Thank you for your continued attention to the issue of Internet freedom. I want to talk to you today about the importance of an open Internet.

An open Internet is what allowed a national broadcaster in Venezuela to upload daily newscasts on YouTube after Hugo Chavez revoked their broadcasting license because their opinions ran counter to his policies.

An open Internet is what ensured the publication of blog reports, photos, and videos of hundreds of Burmese monks being beaten and killed in 2007, even after the government shut down the national media and kicked out foreign journalists.

An open Internet is what brought the protests following the Presidential elections in Iran last summer to all of our attention, even after the government banned foreign journalists, shut down the national media, and disrupted Internet and cell phone service.

But the continued power of this medium requires a commitment from citizens, companies, and governments alike.

In the last few years, more than 25 governments have blocked Google services, including YouTube and Blogger. The growing problem is consistent with Secretary Clinton's recent speech on Internet freedom, in which she cited cases from China to Tunisia to Uzbekistan to Vietnam. For example, our video service, YouTube, has been blocked in Turkey for nearly 2 years now because of user videos that allegedly insult Turkishness.

In 2009, during elections in Pakistan, the Pakistani Government issued an order to all of its ISPs to block certain opposition videos on YouTube. And, of course, there is our experience in China where the last year showed a measurable increase in censorship in every medium, including the Internet.

An open Internet, one that continues to fulfill the democratic function of giving voice to individuals, particularly those who speak in dissent, demands that each of us make the right choices to support a free and strong Internet and to resist government censorship and other acts to chill speech, even when that decision is hard.

As Google's deputy general counsel, part of my job is handling censorship demands from around the world guided by three principles: maximizing access to information on line, notifying users when information has been removed by government demand, and retaining our users' trust by protecting privacy and security.

No example has received more attention than China in recent months. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure, originating from

China with a primary but unsuccessful goal to access Gmail accounts.

However, it soon became clear that what at first appeared to be solely a security incident, albeit a significant one, was something quite different. Other companies, from a range of businesses—finance, technology, media, and chemical—were similarly targeted. We discovered in our investigation that the accounts of dozens of Gmail users around the world who advocate for human rights in China appear to have been accessed by third parties. Let me be clear that this happened independent of the attack on Google, most likely through phishing or malware placed on those users' computers.

These circumstances, as well as attempts over the last year to limit free speech online, led us to conclude that we are no longer comfortable censoring our search results in China. We are reviewing our business operations there now. No particular industry, much less any single company, can tackle Internet censorship on its own. Concerted collective action is needed to promote online free expression and reduce the impact of censorship.

We are grateful for lawmakers, and particularly your leadership, Mr. Chairman, who have urged more companies to join the Global Network Initiative. As a platform for companies, human rights groups, investors, and academics, GNI members commit to standards that respect and protect users' rights to privacy and freedom of expression. Additional corporate participation will help the GNI reach its full potential.

Beyond the GNI, every one of us at the grass-roots, corporate, and governmental level should make every effort to maximize access to information online. In particular, Government can take some specific steps.

First and foremost, the U.S. Government should promote Internet openness as a major plank of our foreign policy. The free flow of information is an important part of diplomacy, foreign assistance, and engagement in human rights.

Second, Internet censorship should be part of our trade agenda because it has serious economic implications. It tilts the playing field toward domestic companies and reduces consumer choice. It affects not only U.S. and Internet companies but also hurts businesses in every sector that use the Internet to reach their customers.

Third, our Government and governments around the world should be transparent about demands to censor a request for user information or when a network comes under attack. This is a critical part of the democratic process, allowing citizens to hold their governments accountable.

Finally, Google supports the commitment of Congress and the administration to provide funds to make sure people who need to access the Internet safely get the right training and tools.

I want to thank each of you for your continued leadership in the fight against online censorship. We look forward to working with you to maximize access to information and promote online free expression around the world.

Chairman DURBIN.

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

Chairman DURBIN. Thank you, Ms. Wong.
Ms. MacKinnon.

**STATEMENT OF REBECCA MACKINNON, VISITING FELLOW AT
THE CENTER FOR INFORMATION TECHNOLOGY POLICY,
PRINCETON UNIVERSITY, PRINCETON, NEW JERSEY, AND
CO-FOUNDER, GLOBAL VOICES ONLINE**

Ms. MACKINNON. Thank you, Mr. Chairman, for the chance to testify today. I look forward to answering your questions along with those of other esteemed members of this Subcommittee.

After describing how authoritarianism is adapting to the Internet—in ways that involve companies, I am afraid—I will offer some policy recommendations.

Now, authoritarian regimes accept these days that they need to connect to the Internet in order to be economically competitive. But they are also working out how to control things well enough to stay in power. Regimes like China and Iran and a growing list of others usually start with the blocking of websites, but they also use a range of other tactics outlined in greater detail in my written testimony. They include cyber attacks against activist websites, deletion of online content by Internet companies at government request, and the use of law enforcement demands in countries where the definition of “crime” includes political speech, which means that companies end up assisting in the jailing and tracking of activists, whether or not they had ever intended to do so.

So what do we do? At the top of my list of recommendations is corporate responsibility. Mr. Chairman, your recent letters to 30 companies in the information and communications technology sector were an important step in advancing the conversation about how American companies can compete in the global marketplace while at the same time upholding core values of Internet freedom.

Soon after your 2008 hearing on this subject, Google, Yahoo!, and Microsoft launched the Global Network Initiative, a code of conduct for free expression and privacy, in conjunction with human rights groups, investors, and academics, including myself. The GNI recognizes that no market is without its political difficulties or ethical dilemmas. Every company, every product, and every market is different. Therefore, we believe in an approach that combines flexibility with accountability. But, fundamentally, it is reasonable, I believe, to expect that all companies in the information and communications technology sector should acknowledge and seek to mitigate the human rights risks and concerns associated with their businesses, just as they and other companies consider environmental risks and waiver concerns.

Next comes legislation. Law may be needed to induce corporate responsibility if companies fail to take voluntary action. Meanwhile, however, I recommend some immediate steps.

It should be made easier for victims to take action in a U.S. court of law when companies assist regimes in violating their universally recognized rights. We need to incentivize private sector innovation that helps support Internet freedom.

We need to revise export controls and sanctions in two ways. On the one hand, we need to fix laws that now make it difficult for U.S. Internet companies to legally serve activists from sanctioned countries like Iran, Syria, and Zimbabwe. Yet, on the other hand, we have to make collaboration with repression more difficult by making it harder for U.S. companies to sell products and services to regimes with a clear track record of suppressing peaceful political and religious speech.

Then there is technical support. Congress deserves great praise for supporting the development of tools that help people in repressive regimes get around Internet blocking. But these tools do nothing to counter other tactics regimes are now using. So our support should also include tools and training to help people evade surveillance, detect spyware, and guard against debilitating cyber attacks; mechanisms to preserve and redistribute censored content that has been deleted from the Internet; and also support for global platforms through which citizens around the world can share information and tactics to fight Internet freedom in innovative ways.

Finally, it is vital that we have continued executive branch leadership. Secretary of State Clinton's landmark speech on Internet freedom made it clear that this is a core American value. In reviving the Global Internet Freedom Task Force, the administration can coordinate between Government and industry and between Government agencies so that U.S. diplomacy, trade, commerce, and national security all can support the goal of Internet freedom.

In conclusion, there is no "silver bullet" for global Internet freedom. As with physical freedom, Internet freedom requires constant struggle and constant vigilance. We will also need a supportive ecosystem of industry, Government, and concerned citizens working together.

Mr. Chairman and all other members of the Subcommittee Chairman Durbin, I commend you for taking the historic first steps in that direction. Thank you.

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

Chairman DURBIN. Thank you very much.

Mr. MEMARIAN. If you would please—thank you.

STATEMENT OF OMID MEMARIAN, IRANIAN BLOGGER, SAN FRANCISCO, CALIFORNIA

Mr. MEMARIAN. I welcome this opportunity to speak on the important matter of Internet freedom, and I hope that our efforts help people around the world to have more access to information via the Internet and the other means of communication.

I am a journalist and a senior researcher for the International Campaign for Human Rights in Iran, an independent nonprofit that monitors Iran's compliance with international human rights standards.

In 2004, I was arrested by the Iranian security forces, and I was held in a prison and in a solitary confinement. Then I was taken to Evin prison, where hundreds of political prisoners—journalists, civil society activists—are being kept after the June 12th Presidential election. During my time in solitary confinement, I was beaten and psychologically and physically tortured repeatedly, and

I was told that I cannot post my writings on my blog and I should stop working as a journalist. There was no actual crime in my case; I was arrested and abused for using the Internet to share information. Just last year, the blogger Omid Mirsayyafi died in detention.

When I moved to the United States in 2005, I learned that my website had been shut down. Don't get me wrong. It was not the Iranian Government who shut down my website. It was a company that provided the domain and host for me. In a letter, the company mentioned the restriction on any transaction with Iranian companies. Later I learned that many pro-democracy and pro-human rights websites had to change their domain on account of that restriction. Anyway, it is very easy for the Iranian Government to monitor dot.ir domains.

When I decided to participate in this hearing, I talked to many of my friends who are bloggers or journalists, and those who have difficulties to even send a simple e-mail or chat on, for example, Yahoo! Messenger. Almost all of them believe that any kind of support to give Iranians more access to the Internet is supporting human rights and democracy in the country, supporting security in the Persian Gulf region, and more importantly, saving the lives of many people who are threatened by restrictions on information that allow the Iranian Government to operate behind closed doors as it violates their basic rights.

As a journalist and a human rights defender, I would like to stress the importance of applying standards in a balanced—not political—way. Not only Iran but numerous other countries violate the right to access the Internet, as the other people today mentioned. And the United States should support compliance across the board. Otherwise, the charge of holding double standards will stick.

So with that in mind, I would like to make four main points in my testimony this morning in relation to global Internet freedom: First, modifying the U.S. sanctions on Iran.

Certain sanctions or interpretations of the sanctions have seriously damaged the ability of Iranians to access the Internet and need to be modified. All mass market software that is useful for publishing, communications, and education should be exempted from the sanctions.

Second is the European companies who still sell surveillance or censorship technology to the Iranian Government need to be exposed and face sanctions. Also, online advertising is not allowed for Persian websites. Many companies, such as Google or Facebook, do not include Persian or Farsi as a supported language for online advertising websites or allow targeting users with such a language.

Also, funding is needed to allow hiring a limited number of web developers in Iran. Many of these small activist groups need to hire developers to be at their websites. The number of web developers with the command of the Persian language outside of Iran is very few. These groups need to be allowed to hire web developers in Iran. The amount of payments could be capped to \$10,000 per year to make sure such a solution is not abused for other purposes.

And I have some other suggestions in regard to internal access and giving VPN accounts to the activists and using anti-jamming for satellite broadcasts. As you know, for Iranian broadcasts, the

U.S. Government could dedicate a specific satellite which is hardened against the jamming using technologies similar to military satellites. And also providing the Iranians with free satellite Internet, which is technologically possible. E-mail security, which is very important, I think there are companies that can provide those kind of technologies. And also PC security, which is another idea, but we can discuss it later.

Thank you.

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

Chairman DURBIN. Mr. Memarian, thank you. We have had a number of witnesses before this Human Rights Subcommittee who have inspired us to continue our work, and you are one of them. You have paid a heavy price for your commitment to your profession of journalism and for your commitment to free expression.

Mr. MEMARIAN. Thank you.

Chairman DURBIN. And your courage to come here today is inspiring to all of us, so thank you very much for doing that.

I can recall the not too distant past when my mother's homeland of Lithuania was finally seeking freedom and independence, and what kept us alive in the United States was the information that came from Lithuania during those dark and dangerous times over fax machines. Well, that was the technology of the moment, and the Soviets could not stop us. And we were kept up to speed on what was happening on a day-to-day basis, and we were able to respond in the global media.

Well, technology has grown in so many different ways, but it still is the right avenue, as Ms. Wong has said, for us to seek it and use it to promote dialog and expression and freedom, which you have sacrificed so much for personally.

In the course of your testimony, you talked about the European companies who sell surveillance or censorship technology to the Iranian Government. As a result of U.S. sanctions against Iran, U.S. companies are not allowed to sell that kind of technology to the Iranian Government. Do you think the U.S. Government should make certain American companies do not sell surveillance or censorship technology to other countries that censor the Internet, such as China or Vietnam?

Mr. MEMARIAN. I think it is very important to include other countries as well, because as some of these countries—Iranians provide those kind of technologies through a third country. So that kind of technology could go to Iran through China or the other countries that have a good relationship with Tehran.

Chairman DURBIN. I suppose after the election that took place 9 months ago, there was the expectation that this so-called Twitter Revolution in Iran would topple the government and change Iran. And obviously that has not occurred, and we have seen the limits of this activism in Iran. But can you give us your view of what impact this had and continues to have in inspiring those who question the current government?

Mr. MEMARIAN. I think if it was not the Internet, God knows how many more people would have been killed on the streets of Tehran and the other cities. And so it has been really important that peo-

ple could document their narratives of the event after the election. So it was very significant.

Chairman DURBIN. I think Ms. Wong made that point as well, and I would like to ask you, you saw the introduction here of Google China and the reference to Tiananmen Square, and I know that your company has announced a change in terms of censorship in China. Can you tell me what your timetable is to accomplish that? If you would turn your microphone on, please. Thank you.

Ms. WONG. Thank you, Senator, and it is a very fair question so let me take it on directly. We do not have a specific timetable. Having said that, we are firm in our decision that we will not censor our search results in China, and we are working toward that end.

We have many employees on the ground, some of whom are very dear colleagues of mine. And so we recognize both the seriousness and the sensitivity of the decision we are making, and we want to figure out a way to get to that end of stopping censoring our search results in a way that is appropriate and responsible. And so we are working on that as hard as we can, but it is a very human issue for us.

Chairman DURBIN. Thank you for stating your clear goal, and I think we are all sensitive to the fact that there are important steps to reach that goal that we want you to make in the right way, in an expeditious way but one that is sensitive to those elements.

Earlier I spoke to the panel, the first panel, about this gradation of cooperation between a company like yours and the government, and I went through a list of possible activities on the Internet, asking where we would draw the line: cooperation with the government to stop child pornography, cooperation with the government in dealing with non-specific politically threatening language, cooperation with the government for specific threats of violence over the Internet, cooperation with the government when there is evidence of advocacy of terrorism, and cooperation when it comes to the disclosure of information classified as secret by that government.

You are on the firing line here when it comes to this issue and the legal questions you have to face. How would Google address these? And how would you draw the lines?

Ms. WONG. Senator, that is a very insightful observation because it is actually something that we wrestle with, and it is incredibly difficult not only to look at a specific piece of content, but to look at it in the context of the country where you are operating. And I think there are multiple layers at which you try and address it. The first is making decisions about entry into a market in the first place, about what frameworks of law that you have to work with. And then when you look at particular pieces of content, you try and make decisions based on what you know about the laws in that country, some of which, like you say, there seems to be almost universal agreement on child pornography as bad, and then on the other extreme very heavy-handed political censorship.

Our general solution is to try and figure out which laws are appropriate for us to abide by given the values of our company and the laws that—or the places where we operate. The second part of that solution is one that Mr. Weitzner commented on, which is transparency. In every jurisdiction where we are required to re-

move information, we try to be transparent with our users that information has been removed to comply with government laws. For example that in China where, when we remove search results from our dot.cn property, we actually put a notice at the bottom of that search result page to let users know that information has been removed as required by law. We do that on all of our services, and in most of our services, what we actually do is link to the demand letter that asked us to remove the information so that the user can see exactly who requested it and what was requested to be removed.

Chairman DURBIN. I would like to follow up and ask about two elements:

The element of due process in these countries. If you are to challenge a government and their assertion of the right to know the name of the user or to censor information, do you use due process in that country to follow their laws?

And, second, can you turn to any international organizations that establish standards that you try to stand by beyond GNI?

Ms. WONG. Sure. Well, yes, we do try to use the legal processes within the country to address—to challenge either requests for user information or censorship demands when we think appropriate. We have done that in Turkey, for example. What that has gotten us is being blocked in Turkey for the last 2 years. In addition, you know, we are looking in terms of our own standards at the GNI principles, but principles that are based on the Universal Declaration of Human Rights. And it is along those lines that we are trying to ensure the maximum amount of access to information.

Chairman DURBIN. If Senator Franken would allow me to ask one more question, and I will not need a second round, and I will then defer to him. But, Ms. MacKinnon, let me ask you about the GNI. I find it interesting that after 2 years we have three active participants and some flirtation and some ignoring of the operation. What is holding them back? I mean, it cannot be money because I put the fee schedule in the record here. It is certainly a reasonable fee, \$2,000 for a company with \$100 million in revenue. It does not sound like a lot of money, although some use that as an excuse. Is there something else that you need to tell us, that you can share with us about this resistance to make this an American effort or an international effort?

Ms. MACKINNON. Mr. Chairman, that is a very good question, and a question I often ask myself. What is holding these companies back? And it does seem in part a fear of acknowledging that human rights is part of their business, that telecommunications and Internet companies, no matter how you slice it, have implications for free expression, privacy, and human rights. And I think a lot of companies are afraid of even having that conversation for fear that people will then hang charges on them of various kinds and that they would rather just avoid having the conversation at all.

I think what we saw with Google, Yahoo!, and Microsoft was an evolution of self-awareness and a real coming out in terms of recognizing it is OK to have this conversation, it is OK to recognize that you have responsibilities, and, in fact, if you hold yourself accountable, that this is good for your business because your users are more likely to trust you, and that if you do make mistakes, there

is a process by which you can try and figure out how to reverse them through a multistakeholder group that is trying to help you succeed.

The point of GNI is not for the human rights groups and the academics like myself in the process to play “gotcha” with the companies, but to really help them avoid making the mistakes by anticipating and thinking through in advance. But the first step is acknowledging that you are not perfect, that you are fallible, that you might even be corruptible as a human being in the pursuit of profits, and that you need help from society and from a range of actors to help do the right thing.

And just as it took quite a while, I think, for industry over time to recognize they had to have public conversations about environmental issues—that took a few decades—and adhere to labor standards—you know, 100 years ago, it took a certain process for companies to be comfortable discussing these things in public, and it has really only been the past few years that companies in this sector have been confronted with this reality that just because you are connecting people to the Internet does not mean you are automatically going to free them, that you have responsibilities in terms of how you are setting up your business and how you are constructing your relationships with different governments and that that matters.

So Google, Yahoo!, and Microsoft are to be commended for making the first step, and I really do hope that other companies will recognize that this is not as scary as it may seem to them and that it is really essential for the future of their business and their credibility, in addition to being the right thing to do if they want a free and open Internet to continue to exist.

Chairman DURBIN. I am going to close with this question, which you may need to think about, maybe not. Let us assume that you are a customer or a user of Facebook, Twitter, Apple, Hewlett-Packard, companies that are not part of this conversation. How could you, if you were a customer or user who happens to believe they should be part of this human rights effort, most effectively influence them through the Internet?

Ms. MACKINNON. Well, certainly there are all kinds of online activist tools, some of which are—you know, you can form Facebook groups, of course. But I think part of it is for customers and consumers and users to really think of themselves as citizens of the Internet and, look, you need to push these companies and services that you are using to do the right thing, you need to be active. And also investors should be thinking about, OK, when I am investing in stock of these different companies, this should be one of the criteria that I am using in addition to their environmental and labor behavior and also when you are thinking of buying products and so on.

So there is a whole bunch of different ways to do this, but part of it is absolutely for consumers to be talking about this, to be putting pressure and saying this company is good, I can trust these people, and these people I am not so sure if I can trust because they are in denial about whether or not there are even any issues about my privacy.

Chairman DURBIN. My guess is before we adjourn this hearing, there will be something underway, and I thank you for your testimony and you, Senator Franken, for your patience.

Senator FRANKEN. Thank you, Mr. Chairman.

I would like to follow up on that because—I think the Global Network Initiative is a great start, but—and this is for both you and Ms. Wong, and, Mr. Memarian, I want to get to you, and I cannot tell you how much admiration I have for your work and your courage.

I think GNI is a great start, but Microsoft is one of the members and Yahoo! is one of the members, and I do not see them making the same kind of decision that Google has made. I think that Bill Gates recently called Chinese censorship very limited. I think those were his words. So what do you think we can do and others can do to help other companies follow Google's lead in China? And that is both to you, Ms. Wong, and you, Ms. MacKinnon.

Ms. WONG. I want to be clear that our decision about China was not an easy one. And I do not think for any company that will confront how to do business in these regimes it is an easy one. We think we have now made the right decision. We stand by our decision for sure. I was frankly kind of puzzled by Microsoft's statements because they are not consistent at all with the conversations we have had over the last 3 years, and in our view, you know, the censorship in China is a human rights issue. It is not to be minimized.

Having said that, I think we have been very clear all through the GNI process that we are not striving for one-size-fits-all solutions. This is the right decision for Google. We would not propose that—impose our decision on any other company, and we do think it is important that they be part of a conversation where we actively discuss how things are going in a country, and that is an important part of GNI.

Ms. MACKINNON. Just to follow up on that, within the GNI, certainly after the CEOs of Microsoft and some other companies made some remarks that were quite disappointing, we had some rather heated discussions internally about that. But it is absolutely true, as Nicole said, it is not one size fits all, that each company has a very different kind of business going on in China. Yahoo! actually sold their Chinese business to a Chinese company a few years ago and do not actually have operational control over that anymore. Microsoft's situation is also somewhat different.

So the idea is not to impose a one-size-fits-all set of standards on everybody in a very rigid way but, rather, to help the companies be mindful about what decisions they are making and what the implications are and to be transparent and accountable about those decisions, because part of the problem—and Senator Durbin alluded to this—is these companies are in China, they have to comply with certain law enforcement decisions, but how are you complying with them?

And so it is an issue of to what extent do they feel comfortable that they are complying in a way that is transparent and responsible and that they can do that within the context of that particular market. And it may be possible for one company to do it and not

another, depending on the very specific relationship they have with the government and the very specific nature of their product.

It is also the case that Google over the past year in China has come under tremendous pressure from the government and in the Chinese media under the guise really of an anti-pornography crackdown, that they have been slammed in the Chinese media for exposing Chinese youth to smutty content when, lo and behold, you type smutty terms into the search engine, smutty results appear.

And so, you know, a lot of these crackdowns and so on are done under the guise of law enforcement and language that we use in the West in a very different context. And so there are very difficult decisions that companies have to make. Oftentimes it is very specific to that company, and the point of the GNI is to be flexible and accountable at the same time. And next year is going to be the first year where we do our first set of evaluations where we start being able to benchmark how the companies have done so far, and that will also help move the process forward.

But it is definitely important to get more companies recognizing, stepping up and taking responsibility. And the GNI is not about, you know, engage or disengage. The fact is that there are a lot of different ways in which you can engage. It is about how you engage rather than in or out.

Senator FRANKEN. Thank you. China is a big market. That is my guess. And you brought up the issue of companies wondering, doing self-examination and talking about how corruptible they are. And I suppose if you are looking at potentially the world's biggest market and taking yourself out of it on a matter of principle, you are making a big decision about how corruptible or incorruptible you are.

Mr. Memarian, thank you for your integrity, your incorruptibility. In your testimony you talk about what is keeping us from having a greater expansion of freedom of speech online in Iran, and rightfully so. But I have a different question, and then I might even go over my time, too, Mr. Chairman. Can you tell us what technological tools Iranians are using right now to get past government censors and surveillance? And I want to know what is already working so that maybe we can do more to support that.

Mr. MEMARIAN. There are companies that provide anti-censorship software so people can go beyond proxies, go behind proxies and have access to the Internet and see those websites that have been filtered. And private companies and initiatives also can provide resources, you know, if you want to do more and provide more access for them, you know, initiatives can provide resources to support the development of technology designed to combat Internet censorship.

I know many people are working on these kinds of software now in San Francisco, in Silicon Valley, and the other States are. So those kind of initiatives could be supported by the States or the State Department or other companies.

I just wanted to add something about the fact that some companies like Yahoo! and Facebook have not joined the GNI initiative. There are many rumors in Iran that Yahoo! and Facebook have made a deal with the Iranian Government and eventually they will give them the information of their users. And the rumors are so

strong in a way that some people have removed their profiles from Facebook because of the threat that they feel.

So I think the fact that Facebook and Yahoo! are not eager to join such initiatives, it is not really acceptable at the time that people are—that really it is a matter of life and death of some people around the world. The world is not suggesting you ask—millions of people in other countries, in Iran, in China, in Vietnam, and Egypt, they use these services and they are really responsible for what they do or what they provide.

Senator FRANKEN. You know, it occurs to me, there was in *Mad Magazine* a series, an ongoing serial cartoon called “Spy vs. Spy,” and this whole thing seems to have an element to it where there is the anti-censorship technology that is being worked on by some people.

Ms. Wong, the Chairman brought this up. In Mr. Memarian’s written testimony, he talked about companies like yours and Microsoft block certain downloads to people in Iran for fear of sanctions. And Mr. Memarian kind of explains that this really just hurts the people of Iran because there is encryption technology that the Iranian Government already has but the people of Iran do not.

So I was wondering in this “Spy vs. Spy” kind of world that we are in here, which includes not just technology but policy, government policy, and business ethics and self-searching, what should we be doing about these kinds of technologies? Do you think that just the government policy here is wrong?

Ms. WONG. I will confess to not being an expert in export control law, but my understanding is that the Office of Foreign Assets Controls has certain regulations that prohibit the download of applications containing encryption, and that is why, in order to comply with those U.S. laws, we do not permit the download of certain applications like our Chrome browser, for example.

Senator FRANKEN. Right.

Ms. WONG. Having said that, our web services are globally available, and we do not prohibit users the access to our websites within Iran. Whether or not there should be a change in those OFAC regulations, I think that totally deserves, just based on the conversation I heard today, some consideration. I know that, for example, some of the regulations are framed according to particular countries. You can have the regulation of not exporting certain things, but exceptions are made, for example, books because we want to have that flow of information and educational materials to a country. Maybe we should start to think about some of the tools that companies like ours provide in that same category of access to information.

Senator FRANKEN. I think Mr. Memarian was basically saying that the Government of Iran already has access to this encryption, so what is the point other than keeping this out of the hands of Iranians. Right?

Mr. MEMARIAN. That is true, and I think that the sanctions are really blanket and should be revised and modified. I understand the concern of those companies which do not risk because the Iranian market is small and these companies prefer to stay away from it. Instead of spending tens of thousands of dollars on legal fees to

apply for an export license, they prefer just to forget it. So if those sanctions would be modified, I think that really helps.

Senator FRANKEN. Well, thank you, Mr. Chairman, for indulging me. Mr. Memarian, thank you for your courage.

Mr. MEMARIAN. Thank you.

Senator FRANKEN. Thank you, Ms. Wong, and thank you, Ms. MacKinnon.

Chairman DURBIN. Thanks, Senator Franken, for your interest in this hearing.

On the last question that you asked, I would submit for the record, and ask that it be made part of the record, a letter from Rich Verma, Assistant Secretary for Legislative Affairs, to Senator Carl Levin which notes that the Department of State is recommending that the Department of Treasury's Office of Foreign Assets Control issue a general license that would authorize downloads of free mass market software by companies such as Microsoft and Google to Iran for personal communication. So our Government is asking for a waiver so that they can provide that additional information.

[The letter appears as a submission for the record.]

Chairman DURBIN. I also have a statement, which I will enter into the record, without objection, from the Chairman of the Committee, Senator Patrick Leahy, as well as statements from Business for Social Responsibility, Computer and Communications Industry Association, the Global Network Initiative, and Reporters Without Borders, which will be entered without objection in the record.

[The statements appears as a submission for the record.]

Chairman DURBIN. I want to thank this panel and the previous panel, two extraordinary panels before this Committee on a critically important topic, brought home by your testimony, Mr. Memarian. You urged us to think about the millions of people around the world looking for a ray of hope each day so that they should continue in their struggle for freedom and find it when they can reach others on the Internet who share their beliefs. This is what made America in its earliest days—Thomas Paine did not have access to the Internet, but his pamphlets were distributed and inspired a lot of people to fight for freedom. You have inspired us, as I mentioned earlier, by coming here today and testifying, particularly about the sacrifice you made in Iran to help that country move forward. I want to thank you for that.

We are going to continue to work on this issue. It may not be 2 years before we meet again, but let us hope that a lot of the companies that refused to be part of this hearing will have second thoughts and will make the right decision to move forward.

This hearing stands adjourned.

[Whereupon, at 11:50 a.m., the Subcommittee was adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

Statement of

The Honorable Richard J. Durbin

United States Senator

Illinois

March 2, 2010

Opening Statement of Senator Dick Durbin
Chairman, Subcommittee on Human Rights and the Law
Hearing on "Global Internet Freedom and the Rule of Law, Part II"
March 2, 2010

This hearing of the Judiciary Committee's Subcommittee on Human Rights and the Law will come to order.

The title of today's hearing is "Global Internet Freedom and the Rule of Law, Part II."

After a few opening remarks, I will recognize Senator Coburn for an opening statement, and then we will turn to our witnesses.

This Subcommittee held our first hearing on global internet freedom in May 2008. At that hearing, we learned that repressive governments around the world censor the internet and persecute human rights and democracy advocates who express their views online. Since then, the scale and scope of internet censorship has increased dramatically.

At our hearing two years ago, I showed some pictures of censored internet searches on Google and Yahoo. Today, I'm going to demonstrate that this censorship continues.

If you go to Google.com and search for "Tiananmen," you will find pictures of the famous Tiananmen Square protests in 1989, especially the iconic photo of a demonstrator standing in front of several tanks.

But if you go to Google.cn, Google's China search engine, and search for "Tiananmen," you will only find beautiful postcard images.

Let me be clear. I'm not singling out Google. Yahoo!, and Bing, Microsoft's search engine, also censor the internet in China. And Baidu, the leading Chinese search engine, censors even more content than these American companies.

I do want to commend Google again for announcing that they plan to stop censoring their Chinese search engine. I look forward to getting an update today on their plans.

At our first hearing, we discussed the Global Network Initiative, or GNI, which was then being negotiated. The GNI is a voluntary code of conduct that requires technology companies to take reasonable measures to protect human rights.

Following the hearing, Senator Coburn and I encouraged Google, Microsoft, and Yahoo! to complete the GNI negotiations, and the code was launched in October 2008. I again want to commend these three companies for taking this leadership role in promoting internet freedom.

Since then, I have asked several dozen other companies to consider joining the GNI. Without objection, the companies' written responses will be entered into the hearing record. They also will be made available on my website.

I am very disappointed that, a year and a half after the GNI started, no new companies have joined.

Based on the responses I received, only three companies, AT&T, McAfee, and Skype, have even committed to participating in a dialogue about joining the GNI. One company, Websense, has indicated that they will join the GNI if the membership fee is waived.

Many companies told me the GNI is not relevant to their company's business. The last two years have shown that simply is not true.

The explosive growth of social networking services, like Twitter and Facebook, has helped human rights activists organize and publicize human rights violations in Iran and elsewhere. However, repressive governments can use these same tools to monitor and crack down on advocates.

I invited Facebook and Twitter to testify today but they refused to appear.

Last year, the Chinese government announced that they would require all computers sold in China to include software called "Green Dam," which censors political content and records user activity.

Thanks to opposition from the U.S. government and companies, the Chinese government eventually backed down. This incident highlighted the human rights challenges faced by computer manufacturers.

I invited Hewlett Packard and Apple to testify about these challenges but they also refused.

Filtering software produced by American companies has allegedly been used to censor the internet in several countries with repressive governments.

I invited McAfee, which produces filtering software, to testify today. McAfee initially agreed to appear, but on Friday informed us that they were pulling out.

The bottom line is this: with a few notable exceptions, the technology industry seems unwilling

to regulate itself and unwilling even to engage in a dialogue with Congress about the serious human rights challenges the industry faces.

In the face of this resistance, I have decided that it is time to take a more active role. At our hearing two years ago, I indicated that Congress could step in if the industry failed to take concrete action to protect internet freedom.

Today I am announcing that I will introduce legislation that would require internet companies to take reasonable steps to protect human rights or face civil or criminal liability. I look forward to working with Senator Coburn and my other colleagues to enact this legislation into law.

I recognize that the technology industry faces difficult challenges when dealing with repressive governments, but Congress has a responsibility to ensure that American companies are not complicit in violating the freedom of expression, a fundamental human right that is enshrined in the 1st Amendment of our Constitution and the Universal Declaration of Human Rights.

tiananmen - Google Search

Page 1 of 1

Web Images Videos Maps News Shopping Gmail more ▾ Search settings | Sign in

Google tiananmen Search Advanced Search
SafeSearch: Moderate ▾

Web Images Show options... Results 1 - 21 of about 648,006 for tiananmen. (0.05 seconds)

Tiananmen Poster
Low Prices on Tiananmen poster Free Shipping on Qualified Orders

Back to top

 Tiananmen-square-studs 630 x 100 - 68k - jpg 240px on web Find similar images	 Tiananmen by James 1600 x 1000 - 177k - jpg about:newsfeeds.wordpress.com	 Tiananmen.jpg 400 x 474 - 97k - jpg rechnerich.net/realworld-worksheets.com	 The Tiananmen 500 x 495 - 70k - gif vintage.kyrgyzstan.com	 Tiananmen Square 340 x 340 - 31k - jpg panther0.com	 from Tiananmen Square 527 x 775 - 40k - jpg geographicalnews.wordpress.com
 Tiananmen Square 400 x 300 - 15k - jpg thebigbigguide.com	 Tiananmen Tower 600 x 350 - 64k - jpg christopher.org	 on Tiananmen Square 474 x 300 - gif old.org	 Interview at Tiananmen 510 x 395 - 38k - jpg hulk.org	 Tiananmen Square 400 x 300 - 33k - jpg chrispictures.org	 Tiananmen 760 x 250 - 18k - gif guardian.co.uk
 the tanks into 264 x 348 - 28k - jpg barbadospress.com	 Tiananmen Square 300 x 300 - 34k - jpg shundafactory.com	 Tiananmen-square-5 350 x 374 - 15k - gif center601.wordpress.com	 Top Decked 300 x 450 - 31k - jpg transpictures.com	 Aerial View of 540 x 480 - 38k - jpg Barnes.org.uk	 Tiananmen-Widow-pid 2040 x 1117 - 358k - jpg st.mirslip.com

1 2 3 4 5 6 7 8 9 10 Next

tiananmen Search

Google Images Home - Report Offenses Images - Help

Google Home - Advertising Programs - Business Solutions - Privacy - About Google

Durbin Sends Letter to Technology Firms Regarding Internet Freedom in China

Tuesday, February 2, 2010

[WASHINGTON, D.C.] – Assistant Senate Majority Leader Dick Durbin (D-IL) today sent letters to 30 information and communications technology companies, including Apple, Facebook, Skype, and Twitter, seeking information about their human rights practices in China following the recent revelation that Google was the subject of a sophisticated cyber-attack in that country. In response to the attack, Google announced it will no longer cooperate with Chinese internet censorship efforts and has threatened to end all Chinese operations.

Durbin, Chairman of the Judiciary Subcommittee on Human Rights and the Law, also announced plans to hold a follow-up hearing on global internet freedom next month. The hearing will feature testimony from Google and other companies about their business practices in internet-restricting countries, as well as from high-ranking Obama Administration officials about the Administration's efforts to promote internet freedom.

"I commend Google for coming to the conclusion that cooperating with the 'Great Firewall' of China is inconsistent with their human rights responsibilities," Durbin said. "Google sets a strong example in standing up to the Chinese government's continued failure to respect the fundamental human rights of free expression and privacy. I look forward to learning more about whether other American companies are willing to follow Google's lead."

Durbin's letter asks each firm for details of its business in China, and what, if any, measures it will implement to ensure that its products and services do not facilitate human rights abuses by the Chinese government.

Today's letter also follows up on a letter that Durbin sent last year, urging technology firms to join a voluntary code of conduct known as the Global Network Initiative (GNI). The code of conduct, which regulates the actions of technology firms operating in countries that restrict the internet, has been backed by Google, Microsoft, and Yahoo!. A copy of last year's letter can be found [here](#).

Durbin sent letters to the following companies:

Companies that responded to Durbin's previous letter: Apple, AT&T, Cisco, Dell, eBay, Facebook, HP, McAfee, News Corp, Nokia, Nokia Siemens, Siemens, Skype, Sprint Nextel, Verizon, Vodafone, Websense.

Companies that partially responded to Durbin's previous letter: Fortinet, Lenovo, Motorola

Companies that did not respond to Durbin's previous letter: Acer, Juniper, Toshiba, Twitter

Companies that did not receive Durbin's previous letter: Amazon, IAC, IBM, Oracle, RIM, SAP

The upcoming hearing will build on Durbin's 2008 hearing examining these issues, at which he questioned Google and Yahoo extensively about their operations in China and urged them to launch the GNI. More information about that hearing can be found [here](#).

The text of the letters appears below:

January 29, 2010

Mark Zuckerberg
CEO and Co-Founder
Facebook
1601 S. California Ave.
Palo Alto, CA 94304

Dear Mr. Zuckerberg,

Thank you for responding to my letter of August 6, 2009. I write to you again following the recent revelations about a Chinese cyberattack on Google and other companies, and Google's subsequent announcement that it will no longer censor its China search engine.

In response to these developments, which have serious implications for internet freedom in China and around the world, I plan to convene a hearing of the Human Rights and the Law Subcommittee. This hearing will follow up on "Global Internet Freedom: Corporate Responsibility and the Rule of Law," a hearing I held on May 20, 2008, at which Google, Yahoo!, and Cisco were questioned extensively about their human rights practices. In preparation for this upcoming hearing, I would appreciate your response to the following:

- Please provide a detailed description of your company's business in China.
- What are your company's future plans for protecting human rights, including freedom of expression and privacy, in China? Please describe any specific measures you will take to ensure that your products and/or services do not facilitate human rights abuses by the Chinese government, including censoring the internet and monitoring political and religious dissidents.

My hearing will also focus on the Global Network Initiative (GNI), a voluntary code of conduct for internet and communications technology companies that requires participating companies to take reasonable measures to protect human rights. I believe that the GNI has great potential to advance human rights if member companies fully implement the GNI's principles and the GNI's membership is expanded.

Thank you for responding to the questions about the GNI in my August 6th letter. On September 10, 2009, the GNI held an "Open House" for companies interested in the GNI (http://www.globalnetworkinitiative.org/newsandevents/Open_House.php). According to the GNI:

Attendees included companies from the telecommunications, equipment and software manufacturing, and Internet sectors. ... Many companies expressed interest in continuing discussions. The GNI is convening a workstream to explore how the current GNI guidelines can be further developed to assist other companies in their efforts to protect freedom of expression and privacy.

In light of these developments, please respond to the following additional questions:

- Did representatives of your company attend the GNI open house? If no, why not?
- Does your company plan to participate in the GNI workstream? If no, why not?

I would greatly appreciate your response to these questions no later than February 19, 2010.

Sincerely,

Richard J. Durbin

January 29, 2010

Jeffrey Bezos
President, CEO and Chairman of the Board
Amazon
1200 12th Avenue South
Seattle, WA 98144

Dear Mr. Bezos,

I write to you following the recent revelations about a Chinese cyberattack on Google and other companies, and Google's subsequent announcement that it will no longer censor its China search engine.

In response to these developments, which have serious implications for internet freedom in China and around the world, I plan to convene a hearing of the Human Rights and the Law Subcommittee. This hearing will follow up on "Global Internet Freedom: Corporate Responsibility and the Rule of Law," a hearing I held on May 20, 2008, at which Google, Yahoo!, and Cisco were questioned extensively about their human rights practices. In preparation for this upcoming hearing, I would appreciate your response to the following:

- Please provide a detailed description of your company's business in China.
- What are your company's future plans for protecting human rights, including freedom of expression and privacy, in China? Please describe any specific measures you will take to ensure that your products and/or services do not facilitate human rights abuses by the Chinese government, including censoring the internet and monitoring political and religious dissidents.

My hearing will also focus on the Global Network Initiative (GNI), a voluntary code of conduct for internet and communications technology companies that requires participating companies to take reasonable measures to protect human rights. I believe that the GNI has great potential to advance human rights if member companies fully implement the GNI's principles and the GNI's membership is expanded.

On September 10, 2009, the GNI held an "Open House" for companies interested in the GNI (http://www.globalnetworkinitiative.org/newsandevents/Open_House.php). According to the GNI:

Attendees included companies from the telecommunications, equipment and software manufacturing, and Internet sectors. ... Many companies expressed interest in continuing discussions. The GNI is convening a workstream to explore how the current GNI guidelines can be further developed to assist other companies in their efforts to protect freedom of expression and privacy.

Please respond to the following additional questions:

- What are your company's views on the GNI?
- Does your company currently follow any of the GNI principles?
- Will your company consider joining the GNI? If yes, please describe the process you will follow to consider joining the GNI. If no, why not?
- Did representatives of your company attend the GNI open house? If no, why not?
- Does your company plan to participate in the GNI workstream? If no, why not?
- Please describe your company's policies and practices for advancing and protecting human rights and minimizing the risk that your products and/or services will facilitate human rights abuses.

I would greatly appreciate your response to these questions no later than February 19, 2010.

Sincerely,

Richard J. Durbin

January 29, 2010

Ken Xie

President and CEO
 Fortinet Inc.
 1090 Kifer Rd.
 Sunnyvale, CA 94086

Dear Mr. Xie,

You did not respond to several questions in my letter of August 6, 2009, and I would appreciate a response at your earliest convenience. I write to you again following the recent revelations about a Chinese cyberattack on Google and other companies, and Google's subsequent announcement that it will no longer censor its China search engine.

In response to these developments, which have serious implications for internet freedom in China and around the world, I plan to convene a hearing of the Human Rights and the Law Subcommittee in February. This hearing will follow up on "Global Internet Freedom: Corporate Responsibility and the Rule of Law," a hearing I held on May 20, 2008, at which Google, Yahoo!, and Cisco were questioned extensively about their human rights practices. In preparation for our upcoming hearing, I would appreciate your response to the following:

- Please provide a detailed description of your company's business in China.
- What are your company's future plans for protecting human rights, including freedom of expression and privacy, in China? Please describe any specific measures you will take to ensure that your products and/or services do not facilitate human rights abuses by the Chinese government, including censoring the internet and monitoring political and religious dissidents.

My hearing will also focus on the Global Network Initiative (GNI), a voluntary code of conduct for internet and communications technology companies that requires participating companies to take reasonable measures to protect human rights. I believe that the GNI has great potential to advance human rights if member companies fully implement the GNI's principles and the GNI's membership is expanded.

In my August 6th letter, I asked you a number of questions about the GNI. Please respond to these questions, which are repeated below for your convenience:

- What are your company's views on the GNI?
- Will your company consider joining the GNI? If yes, please describe the process you will follow to consider joining the GNI. If no, why not?
- Does your company currently follow any of the GNI principles?
- Please describe your company's policies and practices for advancing and protecting human rights and minimizing the risk that your products and/or services will facilitate human rights abuses.

On September 10, 2009, the GNI held an "Open House" for companies interested in the GNI (http://www.globalnetworkinitiative.org/newsandevents/Open_House.php). According to the GNI:

Attendees included companies from the telecommunications, equipment and software manufacturing, and Internet sectors. ... Many companies expressed interest in continuing discussions. The GNI is convening a workstream to explore how the current GNI guidelines can be further developed to assist other companies in their efforts to protect freedom of expression and privacy.

In light of these developments, please respond to the following additional questions:

- Did representatives of your company attend the GNI open house? If no, why not?
- Does your company plan to participate in the GNI workstream? If no, why not?

I would greatly appreciate your response to these questions no later than February 19, 2010.

Sincerely,

Richard J. Durbin

January 29, 2010

Evan Williams
CEO
Twitter, Inc.
539 Bryant St., Suite 402
San Francisco, CA 94107

Dear Mr. Williams,

I am disappointed that you have not yet replied to my letter of August 6, 2009, and would appreciate a response at your earliest convenience. I write to you again following the recent revelations about a Chinese cyberattack on Google and other companies, and Google's subsequent announcement that it will no longer censor its China search engine.

In response to these developments, which have serious implications for internet freedom in China and around the world, I plan to convene a hearing of the Human Rights and the Law Subcommittee in February. This hearing will follow up on "Global Internet Freedom: Corporate Responsibility and the Rule of Law," a hearing I held on May 20, 2008, at which Google, Yahoo!, and Cisco were questioned extensively about their human rights practices. In preparation for our upcoming hearing, I would appreciate your response to the following:

- Please provide a detailed description of your company's business in China.
- What are your company's future plans for protecting human rights, including freedom of expression and privacy, in China? Please describe any specific measures you will take to ensure that your products and/or services do not facilitate human rights abuses by the

Chinese government, including censoring the internet and monitoring political and religious dissidents.

My hearing will also focus on the Global Network Initiative (GNI), a voluntary code of conduct for internet and communications technology companies that requires participating companies to take reasonable measures to protect human rights. I believe that the GNI has great potential to advance human rights if member companies fully implement the GNI's principles and the GNI's membership is expanded.

In my August 6th letter, I asked you a number of questions about the GNI. Please respond to these questions, which are repeated below for your convenience:

- What are your company's views on the GNI?
- Will your company consider joining the GNI? If yes, please describe the process you will follow to consider joining the GNI. If no, why not?
- Does your company currently follow any of the GNI principles?
- Please describe your company's policies and practices for advancing and protecting human rights and minimizing the risk that your products and/or services will facilitate human rights abuses.

On September 10, 2009, the GNI held an "Open House" for companies interested in the GNI (http://www.globalnetworkinitiative.org/newsandevents/Open_House.php). According to the GNI:

Attendees included companies from the telecommunications, equipment and software manufacturing, and Internet sectors. ... Many companies expressed interest in continuing discussions. The GNI is convening a workstream to explore how the current GNI guidelines can be further developed to assist other companies in their efforts to protect freedom of expression and privacy.

In light of these developments, please respond to the following additional questions:

- Did representatives of your company attend the GNI open house? If no, why not?
- Does your company plan to participate in the GNI workstream? If no, why not?

I would greatly appreciate your response to these questions no later than February 19, 2010.

Sincerely,

Richard J. Durbin

Durbin, Coburn Continue to Press Tech Companies on Human Rights Code of Conduct

Friday, August 7, 2009

[WASHINGTON, DC] – Assistant Senate Majority Leader Dick Durbin (D-IL) and Senator Tom Coburn (R-OK) sent a letter today to 26 tech companies, urging them to join a voluntary code of conduct known as the Global Network Initiative (GNI). Recent crackdowns in China and Iran have made the code of conduct, which regulates the actions of technology firms operating in countries that restrict freedom of expression, even more important to the protection of human rights.

Durbin and Coburn, Chairman and Ranking Member of the Senate Judiciary Subcommittee on Human Rights and the Law, held a hearing in May 2008 on the issue of internet freedom and since then have pushed for the establishment and implementation of the tech industry's code of conduct.

"We recognize and appreciate that information and communications technology (ICT) companies have enabled billions of people around the world to express themselves more fully and freely. Iranian opposition protesters' use of the internet is one recent, prominent, and inspiring example. At the same time, recent events in China make clear that repressive governments around the world continue to restrict their citizens' ability to exercise their right to freedom of expression," the Senators wrote.

"We believe the Global Network Initiative has great potential to advance and protect human rights if member companies fully implement the GNI's principles and the GNI's membership is expanded."

American tech companies now operate in many countries where the internet is censored or where governments use technology as a tool to repress their citizens. The result of these efforts is not only the suppression of freedom of speech, but also too often the persecution and imprisonment of those who violate a state's strict internet regulations.

Today's letter urged the companies to sign on to the GNI code of conduct and to work towards its full implementation. Today's letter was sent to the CEO's of the following companies: 3Com, Acer, Apple, AT&T, Cisco, Dell, eBay, Facebook, Fortinet, Hewlett-Packard, Juniper, Lenovo, McAfee, Motorola, MySpace, Nokia, Nokia-Siemens, Siemens, Skype, Sprint Nextel, Symantec, Toshiba, Twitter, Verizon, Vodaphone, and Websense.

Over the last several weeks, Human Rights and Law Subcommittee staff met with each of these companies to discuss the code of conduct, except for three companies that refused to meet: 3Com, Fortinet, and Websense.

A copy of the letter can be found below.

August 6, 2009

Dear Company CEO,

We appreciate [COMPANY NAME] representatives taking the time to meet with staff from the Human Rights and the Law Subcommittee recently about [COMPANY NAME]'s approach to human rights issues.

As the Chairman and Ranking Member of the Human Rights and the Law Subcommittee, we recognize and appreciate that information and communications technology (ICT) companies like [COMPANY NAME] have enabled billions of people around the world to express themselves more fully and freely. Iranian opposition protesters' use of the internet is one recent, prominent, and inspiring example.

At the same time, recent events in China make clear that repressive governments around the world continue to restrict their citizens' ability to exercise their right to freedom of expression. Companies that conduct business in such countries can play a vital role in promoting freedom of expression, but they must not do so at the expense of their users' privacy. While no ICT company can absolutely guarantee that it will not unwittingly facilitate government repression, every ICT company should take reasonable measures to minimize the risk of such complicity.

One promising avenue for reducing exposure to human rights violations is the Global Network Initiative (GNI), a voluntary code of conduct for ICT companies that requires participating companies to take reasonable measures to protect human rights (for more information, see <http://www.globalnetworkinitiative.org>). On May 20, 2008, we held a hearing on "Global Internet Freedom: Corporate Responsibility and the Rule of Law," at which there was extensive discussion about the GNI, which was then being negotiated by, among others, Google, Microsoft, Yahoo!, and leading human rights organizations and socially responsible investment companies.

Following the hearing, we encouraged Microsoft, Google, and Yahoo! to complete the GNI negotiations as soon as possible. On October 28, 2008, the GNI was launched and since that time, the Human Rights and the Law Subcommittee has closely monitored its progress. We believe the GNI has great potential to advance and protect human rights if member companies fully implement the GNI's principles and the GNI's membership is expanded. While the GNI principles are universal, we understand that the GNI is intended to be adaptable to the particular circumstances of companies from all sectors of the ICT industry, regardless of size and geographic location. We also note that if ICT companies do not take reasonable steps to effectively protect human rights, like those contemplated by the GNI, it may be necessary for Congress to consider legislation to ensure that companies take such measures.

Accordingly, we strongly encourage [COMPANY NAME] to consider participating in the GNI.

We would appreciate your responses to the following questions by August 27, 2009:

1. What are your company's views on the GNI?

2. Will your company consider joining the GNI? If yes, please describe the process you will follow to consider joining the GNI. If no, why not?
3. Does your company currently follow any of the GNI principles?
4. Please describe your company's policies and practices for advancing and protecting human rights and minimizing the risk that your products and/or services will facilitate human rights abuses.

Sincerely,

Richard J. Durbin

Tom Coburn



Acer Incorporated
 8F, 88, Ser. 1, Hsin Tai Wu Rd., Hsueh-shan
 Taipei Hsien 221, Taiwan, R.O.C.
 宏碁股份有限公司
 台北市中正區新泰南路一號八八樓
 TEL: 886-2-2696-3131
 886-2-2696-1234
 FAX: 886-2-2696-3535
 www.acer.com.tw

March 1, 2010

The Honorable Richard J. Durbin
 Chairman
 Subcommittee on Human Rights and the Law
 U.S. Senate Committee on the Judiciary
 224 Dirksen Senate Office Building
 Washington, DC 20510

The Honorable Tom Coburn
 Ranking Member

Re: The Subcommittee's Letters of August 6, 2009 and January 29, 2010
Addressed to Acer Inc. ("Acer")

Dear Chairman Durbin and Ranking Member Coburn:

Thank you for the Subcommittee's letters of August 6, 2009 and January 29, 2010 addressed to Acer's CEO and President, Gianfranco Lanci. Mr. Lanci, J. T. Wang (Acer's Chairman of the Board), and I have discussed the letters and the issues they raise in detail, and Mr. Lanci asked that I respond on Acer's behalf. I apologize for Acer not responding more promptly to the questions posed in the August 6, 2009 letter. We greatly respect the Subcommittee's work and address its inquiries below.

The letters raise important and challenging issues of human rights, international law, respect for nations' local laws, international diplomacy, and corporate responsibility. As a company founded in Taiwan, Acer is sensitive to these issues, and we respect human rights throughout our companies' operations.

I. Background On Acer

Acer was founded privately in Taipei, Taiwan in 1976. Since then, it has become a global public company with over 6,500 employees that sells its products in North and South America, Africa, Asia, Europe, and the Middle East. Our primary products are hardware for individuals and businesses: desk-tops; notebooks; handhelds; tablets; servers and storage; LCD monitors; and peripherals.

We have succeeded through a commitment to creating value for our customers, our employees, our investors, and our business partners. Equally so, we have succeeded because we adhere to the core values explicitly set forth in our Standards of Business Conduct. We enclose a copy of these standards for additional information.

These standards emphasize our fundamental mandate to act as good corporate citizens. Specifically, this entails respecting human rights, following the national laws of the many countries in which we operate, respecting community standards and social



Acer Incorporated
8F, 8B, Sec. 1, Hsin Tai Wu Rd., Hsuehshih
Tajpei Hsien 223, Taiwan, R.O.C.
宏碁股份有限公司
台北市223, 新北市新莊區五福一路88號8樓
Tel: 886-2-2695-3131
886-2-2695-1234
Fax: 886-2-2695-3535
www.acer.com.tw

norms, and maintaining high standards for ethics and safety. Our ethical pillar entails three distinct values: (1) playing a role in social growth; (2) caring for the environment across the business value chain; and (3) respecting people, diversity, and cultures. These standards are not just slogans – we train our employees in these policies, and we enforce them.

II. The Global Network Initiative (“GNI”)

We have reviewed GNI’s existing principles, and its core principles of freedom of expression, privacy, responsible company decision-making, and multi-stakeholder collaboration are all important. For example, our Standards of Business Conduct make clear that protecting our customers’ privacy is one of our paramount priorities.

On February 22, 2010, GNI published a document entitled “Issues for Consideration in GNI Implementation,” explaining that the existing principles reflect the circumstances faced by internet and telecommunications firms. The document further explained that additional dialogue was needed to better evaluate how GNI could adapt the existing principles and implementation guidelines to apply to equipment manufacturers such as Acer. Consequently, GNI has initiated an Implementation Dialogue to achieve this objective.

Mr. Lanci and Mr. Wang have instructed me to closely monitor the GNI Implementation Dialog and consider the issues it raises seriously. Unfortunately, neither Mr. Lanci, Mr. Wang, nor I were aware of GNI’s open house last year and an Acer representative did not attend.

III. Questions Regarding China

A. Acer’s Business in China

Acer conducts three types of business in China. First, we sell computer equipment to individuals and businesses. Second, we sell computers to the Chinese government. Third, we provide after-sale services to individuals, businesses, and the government for Acer’s branded computers.

As of the third quarter of 2009, we have a market share in personal computer equipment of 3.3%. Our largest competitors in China are Lenovo, HP, Dell, Asus and Founder Electronics, with respective market shares of 24.3%, 15.4%, 7.4%, 6.6%, and 5.6%. (** Data source: Gartner)

B. Acer’s Approach to China from a Corporate Responsibility Perspective

Per the Subcommittee’s questions, we understand that the Subcommittee and the U.S. government have concerns about China with respect to freedom of expression and



Acer Incorporated
 8F, 88, Sec. 1, Hsin Tai Wu Rd., Hsueh-h
 Taipei Hsueh 221, Taiwan, R.O.C
 宏碁股份有限公司
 台北市221, 新市路九路一段88號8樓
 Tel: 886-2-2696-3131
 886-2-2696-1234
 Fax: 886-2-2696-3535
 www.acer.com.tw

privacy. Preliminarily, we note that, under official U.S. government policy, Acer's base of Taiwan is a part of the People's Republic of China. Thus, any law with which Acer complies in China is considered to be the policy of our own governing nation state.

As a company originally founded in Taiwan, we are particularly sensitive to the differing positions that China, the United States, and other countries take on many issues, including the internet. In accordance with our Standards of Business Conduct, we respect and obey the local laws of the individual countries in which we operate. We apply this principle equally across all our global markets.

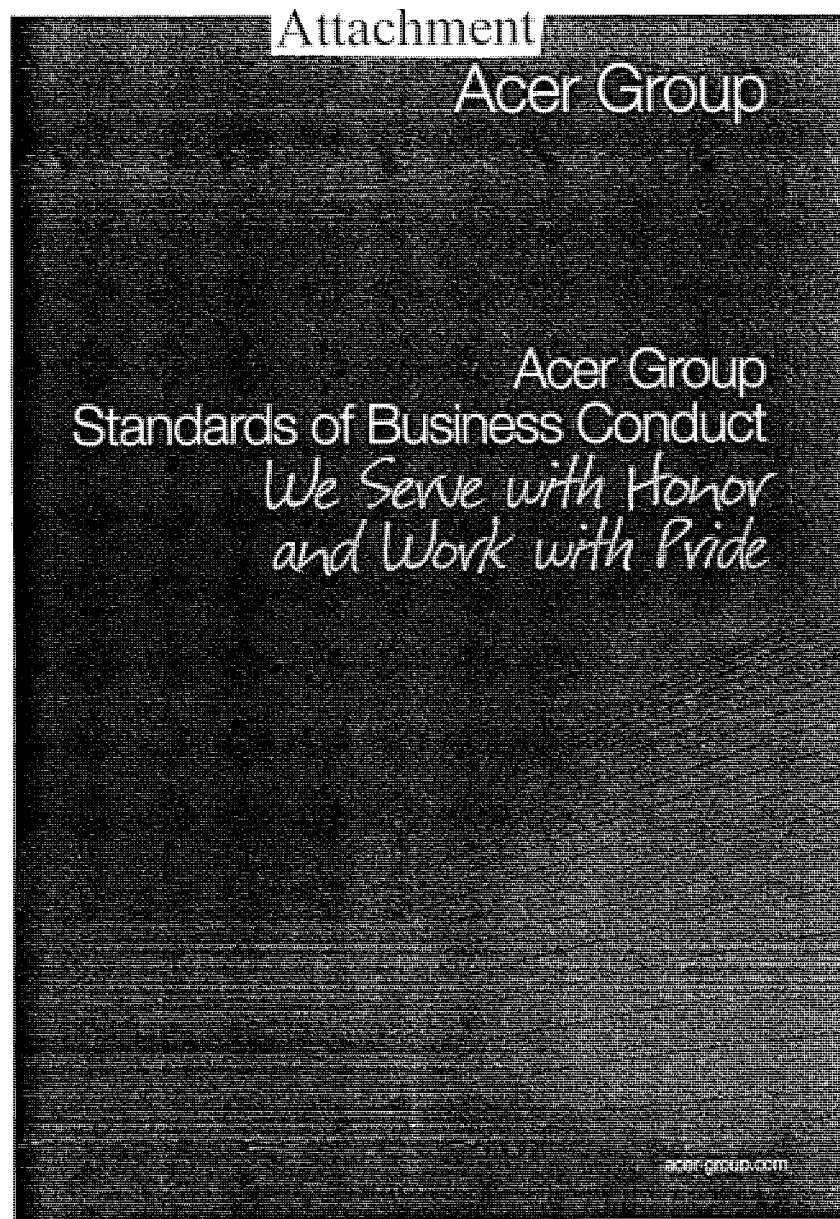
Significantly, as we state in our Standards of Business Conduct, we care deeply about human rights and ensure our company respects them. No government, including China, has ever asked us to do anything outside of its legislative, judicial, or regulatory process. Our customers have always been informed about their countries' policies with respect to our products. We believe that transparency is key to addressing some of the Subcommittee's concerns, and that has never been an issue with respect to our business in any country, including China.

We firmly believe our business operations within China as an ICT company facilitate open discourse, especially as we help bring personal computers to China's rural areas. Bringing personal computers to China's rural areas is a priority for the government, and we are pleased to help it accomplish that objective.

Thank you for including us in your considerations of important public policy questions. We hope you find our response helpful.

Sincerely,

Lydia Wu
 General Counsel



Acer Group

Dear Team,

The vision of the Acer Group to become "A leading branded company empowering and enriching people through innovation and customer care," gets closer to reality when all of us contribute to the common purpose of "Breaking the barriers between people and technology."

Similarly, "Serve with honor and work with pride" is about our core values, which compel us to consistently strive to create value by being innovative, fast and effective.

These core values also drive us to constantly deliver what customers want in an ethical and caring environment.

This is done every day in every decision and every action by each one of us. We continue to build on our reputation for trust, integrity and honesty, both internally and externally, by appreciating people, their diversities and cultures. As good corporate citizens we respect human rights, local communities and compliance with laws, environment, ethics, safety standards, regulations and social norms.

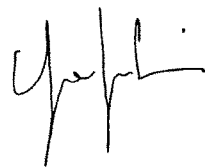
We believe in turning slogans into reality by demonstrating our actions through our core values. Inspired by these values, we have formulated a Standards of Business (SBC) document to guide us on how we interact with each other, our customers, our business partners, our shareholders and the communities where the Acer Group does business.

The reputation and success of the Acer Group around the world always depends on the individual and collective integrity of each one of us.

Hence, we strongly believe "Serve with honor and work with pride" is an integral part of our way of doing business globally. Adherence to the guidance in this document is required by all Acer Group employees around the world. Its implementation needs to be monitored rigorously and managers should ensure that all employees are aware of these principles and abide by them.

Sincerely,

Gianfranco Lanci
CEO & President Acer Inc.



J.T. Wang
Acer Group CEO and Acer Inc. Chairman



Acer Group

*Acer Group Values and
Standards of Business Conduct*

Acer Group Core Values

The Acer Group values are the core beliefs we use as a frame of reference for any organizational decision. They act as a compass that guides us to achieve our mission of "Breaking the barriers between people and technology."

We have organized our core values based on the way we should act and the pillars on which we should base our actions to guide us in conducting business and relating with each other.

The way we must act

INNOVATIVE	
Rational Meaning	Emotional Meaning
Challenging the way of doing things and adopting new ideas	Think big
Supporting continuous improvement in processes and products	Think smart
Creating impact through original thinking	Think out of the box (innovatively)

FAST	
Rational Meaning	Emotional Meaning
Putting speed in execution at the heart of our operations	Think fast
Being proactive in making decisions	Act quickly
Anticipating changes ahead of competition as key to success	Get there first

EFFECTIVE	
Rational Meaning	Emotional Meaning
Doing the right things right	Clear objectives
Creating an empowered environment with clear responsibilities and targets	Clear responsibilities
Recognizing the power of being simple and attentive to the basics	Keep it simple

Acer Group

The pillars on which we must base our actions

VALUE CREATING	
Rational Meaning	Emotional Meaning
Generating profit for our shareholders	Value for shareholders (good dividends and share value)
Growing the business by achieving challenging financial and strategic objectives	Value for customers (good products, services, easy to do business with)
Leveraging on our key assets: brands, people, customers and channel	Value for employees (good company, environment, opportunities)

CUSTOMER-CENTRIC	
Rational Meaning	Emotional Meaning
Recognizing that customers are the essence of our business	Love and respect our customers
Placing first priority on listening and satisfying customer needs	Listen, learn and improve
Delivering first class products and services	Walk the talk (delivering on our promises)

ETHICAL	
Rational Meaning	Emotional Meaning
Being a good corporate citizen by playing a role in social growth	Trust, respect and honesty
Caring for the environment all across the business value chain	Care for the environment
Building on trust and honesty internally and externally by respecting people, diversities and cultures	An example to others

CARING	
Rational Meaning	Emotional Meaning
Creating an attractive workplace and ensuring a proper work-life balance	Energetic and inspiring workplace
Providing employees with development and professional growth opportunities	Growth potential
Fostering teamwork and collaboration	Teamwork

Standards of Business Conduct

It is Acer Group policy to fully comply with all laws and regulations governing our people and operations around the world and to conform to the highest legal and ethical standards.

Our Standards of Business Conduct (SBC) are formulated to guide the way Acer Group employees behave with each other, our customers, business partners, our shareholders and the communities where Acer Group does business.

Should any provision conflict with the local laws or regulations, the one with highest standard under the law will apply.

Our Work Environment is Caring

1. We embrace high standards of ethical behavior and treat all colleagues fairly, with dignity and with respect. One of our core values is "caring".
2. We embrace the diversity and culture of all members of the team and provide a work environment free from discrimination (based on race, color, age, gender, sexual orientation, ethnicity, religion, disability, union membership or political affiliation) and harassment.
3. We fully comply with laws related to working hours, minimum age (no child labor or forced labor) and benefits, and we ensure that all our suppliers comply with these requirements.
4. We provide fair remuneration and always comply with the applicable national statutory minimum wage.
5. We comply with all applicable health and safety regulations to provide all our employees a healthy and safe working environment.
6. We provide facilities, training programs, time and subsidies to support employee creativity and career development.
7. We protect the personal information of employees and the board of directors and respect their privacy and the need to protect their personal information.
8. We ensure fairness in hiring, do not employ or make anyone work against his/her will, and use objectivity in promoting and fairness in terminations.
9. We clearly understand and respect the scope of authority given, and do not autonomously override these parameters.

The customer is the reason for our existence

- We welcome customer opinions and endeavor to develop and improve products and services that satisfy customer needs.

Acer Group

- We promote constant technological innovation and improvement to produce safe, high quality products for our customers.
- We respond to requests and queries of customers in an honest, prompt and appropriate manner.
- We walk the talk (deliver as per the commitment) to earn customer respect and loyalty.
- We provide reliable information to our customers regarding products and services.
- We conduct our sales, service and marketing activities utilizing sound business practices and are fully in compliance with all applicable laws and regulations.

Fair Competition

- We earn our customers' trust through quality and value-adding products and services and through ethical and legal behavior.
- We compete with competitors fairly in compliance with any and all laws and regulations enacted for the purpose of maintaining free and fair competition.
- We do not make untrue statements about our competitors or their products and services.
- We abide by all antitrust laws and regulations. In particular we will not enter into agreements or arrangements with competitors to lower, raise or stabilize the prices of our offerings.
- Likewise, we will not enter agreements or reach understandings with competitors to bid on public or private contracts or to "divide up" markets, territories, customers, product or services or to limit availability of any of our offerings.

Respect for Environment

- We comply with all applicable laws and regulations related to the environment.
- We promote the research and development of advanced technologies, products and services that benefit the environment.
- We support continuous improvements in environmental protection.

Intellectual Property Rights

- We comply with all intellectual property rights laws and regulations, including patents, trademarks and copyrights. We respect the legitimate intellectual property rights of third parties.
- All ideas and inventions conceived by any employee during the term of employment that relate to Acer Group's business are the exclusive property of the Acer Group. This standard applies regardless of whether the employee was acting alone or with others.

Conflicts of Interest

- Employees are prohibited from engaging in any activity, investment or association that creates, or appears to create a divided loyalty between the employee and the Acer Group.

- The best policy is to avoid any direct or indirect business connection with our customers, suppliers or competitors, except on behalf of the Acer Group.
- Employees must disclose any such relationship and refrain from making decisions on behalf of the Acer Group that may have the effect of benefiting an employee personally outside of the employee's scope of employment with the Acer Group.
- We make decisions in the best interest of the Acer Group and refrain from business dealings with outside firms that result in improper gains to outside individuals or entities.
- Employees may not directly supervise or participate in hiring or promotion decisions that affect the employee's spouse, domestic partner or immediate family.
- Questions or concerns about whether a particular circumstance constitutes a conflict of interest should be directed to the Acer Group's Human Resources Department or Legal Department.

Vendors and Other Business Partners

- We offer equal opportunities to all qualified companies and individuals seeking to do business with the Acer Group. Acer Group employs a fair and objective evaluation process in the selection of business partners.
- We pursue cooperation with our business partners in a mutual effort to promote a healthy trading environment and maintain a fair trading system.
- The Acer Group does not engage in discrimination prohibited by law in its selection of business partners.
- We endeavor to do business only with partners that uphold the Acer Group's high standards with regards to ethics, human rights, health, safety and environment and expect all business partners to comply with all relevant laws and regulations as well as with Acer Group Supplier Code of Conduct.

Corporate Communications

- We conduct corporate communications with integrity on the basis of objective facts to enable customers, shareholders, potential investors and employees to obtain a reasonable understanding of Acer Group activities.
- All corporate communications are issued in cooperation with the Acer Group's Corporate Communications Department, including disclosure of business information to analysts, newspapers, magazines, radio, television stations, and all other media.

Advertisements

- We ensure that our advertisements are truthful, accurate and comply with all relevant laws and regulations. Although we may make valid comparisons of our offers to the offerings of

Acer Group

our competitors, we do not unfairly disparage our competitors.

- All advertisements should be created with a sense of responsibility toward the public.
- We do not promulgate advertisements that would be deemed disrespectful or offensive to customers.

Accounting

- We shall comply in full with all laws or regulations regarding accounting and will conduct proper account management and financial reporting.
- All employees are required to promptly report all cases of suspected financial or operational misrepresentation or impropriety.
- We do not make any false or misleading entries in Acer Group's books or records for any reason.

Lenders and export credit compliance

- We conduct our business activities in full compliance with all applicable laws and regulations of the respective countries in which we do business.
- We will disclose all relevant material facts in connection with obtaining financing from an export credit agency or from other lenders.

Financial Interest in other Companies

- While employed by Acer Group, employees cannot invest in or work with customers, suppliers or competitors of the Acer Group except in their capacity as an Acer Group employee.
- Employees must refrain from receiving, or giving the appearance of receiving, improper personal benefits as a result of their position in or affiliation with Acer Group.
- Conflicts of interest may not always be clear. Any exception to Acer Group's conflict of interest standards must be approved by senior management or the Board of Directors.

Prohibition of improper payments

- We observe prohibitions on payments that are illegal or improper under generally accepted sound business practices and local law.
- We will not let business dealings on behalf of the Acer Group be influenced by personal or family interests.

Gifts and Entertainment

- We provide or accept gifts that are reasonable complements to business relationships but not those that may create undue influence--or even the appearance of undue influence--in decision making.

- All employees, regardless of position or responsibility are prohibited from accepting gifts or other items of value that exceed 5% of their weekly salary or 50 US Dollars, from any business relations such as suppliers, customers, or government officials. The limit is decided on economical value and ethical acceptable standards in the recipient's respective country or culture. Consult Acer Group's Human Resources Department or Law Department to address circumstances in which gifts in excess of this amount are received or proposed to be given and it would be against Acer Group's interests to refuse item(s) offered or otherwise adhere to the limit stated herein.
- Customary business amenities such as meals and entertainment may be offered or accepted if at a reasonable level and not prohibited by law or normal business practice. Examples of acceptable entertainment opportunities include attendance at sales events, product launches or professional seminars. The offering or acceptance of gifts and entertainment is strictly prohibited in circumstances where such offering or acceptance violates local law.
- Entertainment expense needs to conform to laws and policies of the country or region where the expenses are incurred. Employees are expected to be mindful of their and Acer Group's image, and hence exercise good judgment in the choice of gifts and entertainment and make choices which are in good taste and which will not embarrass the Acer Group or the other party.

Protection of Company assets

- We use company assets only for legitimate business purposes and not for personal benefit.
- All assets should be handled appropriately and with care to avoid loss, theft or damage. This includes physical assets, intellectual property rights, and information assets.
- The Acer Group name, logo, information, equipment, property, time and other resources may not be used to engage in outside activities which have not been sanctioned by the Acer Group.
- Employees must only utilize the company's computer network system and other IT resources for legitimate business purposes, must observe IT security requirements and must refrain from utilizing such resources for unethical or illegal purposes.

Confidential Information

- Employees are expected to safeguard all or any confidential information pertaining to Acer Group companies or business units and not use such information for personal benefit or in a manner that would harm Acer's interests, either during or after employment.
- We take care to protect the confidential and proprietary information with which we are entrusted by our current and former employees, customers and suppliers.
- We use personal data only for appropriate purposes and protect personal data in accordance with all applicable laws, regulations and company rules.

Acer Group

Insider Trading

- Inside information is information not readily available to the public that an investor would consider important in deciding whether to buy or sell a company's stock. Examples of inside information include unannounced mergers and acquisitions, unannounced product strategies, marketing plans and vendor contracts.
- We are not allowed to share "inside" information (that is not known to public) with anyone other than people with a legitimate business need to know within the Acer Group companies or business units and who have agreed or otherwise have an obligation to safeguard the information.
- All non-public information must be used only to further the Acer Group's legitimate business interests and not for any undue advantages or personal gains.

Drugs and Alcohol

- During legitimate business entertainment or other Acer Group events where consumption of alcohol is authorized, we will ensure that our alcohol consumption is moderate and at reasonable levels. We take care to ensure the use of alcohol does not create a safety risk.
- We do not sell, possess or use illegal drugs.

Political Contributions and Activities

- The Acer Group does not make contributions to political parties or committees, unless permitted to do so by applicable laws, regulations and company rules and such contributions are deemed appropriate and authorized by senior management.

Community Relations

- We actively participate in developing communication with the local community to encourage and maintain mutual respect and understanding.
- We undertake all activities in harmony with the community, by respecting the local culture and community traditions and customs.
- We actively participate in social and community activities, and voluntary services.

Business Travel

- All business travel must be for legitimate business purposes and must be in accordance with the Acer Group's regional/country travel policy.

Membership on Corporate Boards or Advisory Committees

- Employees must ensure that their membership on corporate boards or advisory committees does not, either directly or indirectly, conflict or create the appearance of conflicting with their responsibilities as an Acer Group employee.

Making the Right Choices,
Seeking Guidance and Reporting Suspected Violations
**If you are unsure about a decision,
ask yourself the following questions:**

1. Is it legal and ethical?

2. Does the action comply with Acer Group values, policies, and guidelines?

3. Would I feel comfortable telling my managers, colleagues or other people who are important to me about the decision?

4. Would I feel comfortable if the decision was published in the newspaper?

**If the answer to any of the above is “NO”,
simply, do not do it!**

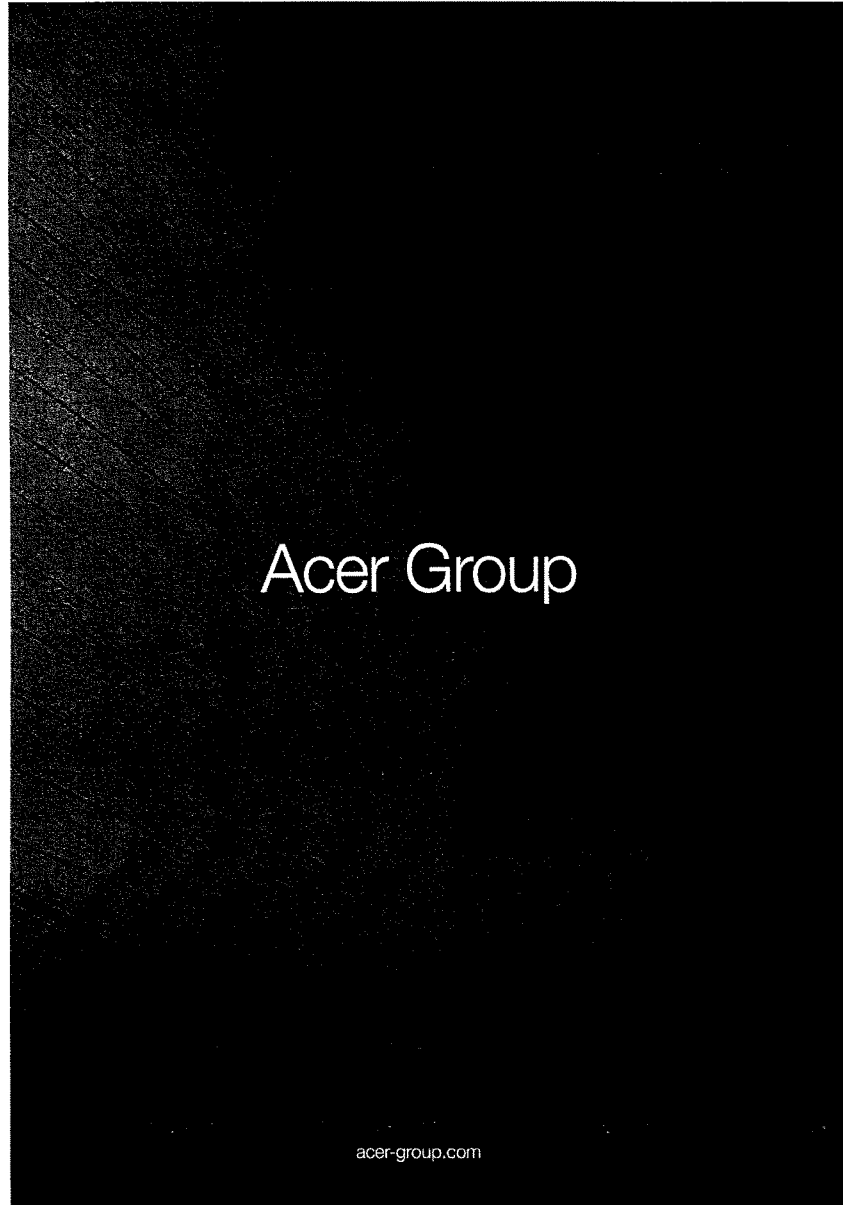
The Acer Group Standards of Business Conduct supersedes all other company policies, procedures, instructions, practices, rules and verbal representations to the extent they are inconsistent or less restrictive than the Acer Group Standards of Business Conduct. Acer Group business units may, however, adopt procedures that are more restrictive than these Standards or may issue modified rules if necessary to comply with local law. Any violation of these Standards or violation of applicable laws or recognized ethical business standards will subject every involved employee at any level to disciplinary action up to and including termination.

If you have a question about what constitutes a breach of the Acer Group Standards of Business Conduct, if you see or hear about illegal or unethical conduct affecting the Acer Group or you are aware of somebody doing something dishonest, destructive, illegal or otherwise not in the Acer Group's best interests, contact Acer Group management, the Acer Group Human Resources Department or the Acer Group legal Department. Such contacts may be made formally (such as by letter) or informally (such as by having an informal discussion about your concern with your supervisor).

All reports are treated confidentially. No retaliation will be undertaken against individuals who report suspected violations in good faith and the identity of those making such reports will be protected to the extent consistent with the law and Acer Group policy.

Acer Group

*Serve with Honor
and Work with Pride*





HAND DELIVERED

February 18, 2010

Honorable Richard J. Durbin
United States Senate
Hart Senate Office Building Room 309
Washington, DC 20510

Dear Senator Durbin:

Thank you for your letter of January 29, 2010, regarding Amazon's business in China.

Amazon opened on the World Wide Web in July 1995 and today offers millions of unique items in categories such as Books; Movies, Music & Games; Digital Downloads; Electronics & Computers; Home & Garden; Toys, Kids & Baby; Grocery; Apparel, Shoes & Jewelry; Health & Beauty; Sports & Outdoors; and Tools, Auto & Industrial. Amazon, in conjunction with its overseas affiliates, operate websites, including www.amazon.com, www.amazon.co.uk, www.amazon.de, www.amazon.co.jp, www.amazon.fr, www.amazon.ca and, primarily for Chinese customers, www.joyo.com or www.amazon.cn.

Most of the overseas businesses are operated locally, largely with local employees and managers, and offer products and services sourced largely from the region (e.g., chosen and purchased from regional vendors), and are designed for and cater to local consumer needs, cultures, languages, currencies, and laws. These overseas websites are retail destinations and, as a general matter, do not offer communication services to customers. Thus, in China, for example, we do not operate a network or Internet search engine.

Our business in China has its roots in Joyo.com, which was founded in 2000. In 2004, when Amazon acquired Joyo.com Limited, the Joyo.com website was already one of the leading online shopping platforms in China and was rebranded as "Joyo Amazon" in 2007. Today the site offers customers hundreds of thousands of items in 22 categories including electronics, media, watches, mother/baby products, kitchen, and health/personal care.

Joyo Amazon provides COD delivery to hundreds of cities throughout China, and same-day delivery to customers in Beijing, Shanghai, and Guangzhou. There are four fulfillment centers: in Beijing; in Suzhou (in the southeast, about 100 km from Shanghai); in Guangzhou (in the south, near Hong Kong); and in Chengdu (to the southwest -- the capital of the Sichuan province).

The Beijing fulfillment center is the largest, at 40,000 square meters. It can hold 12 million items, and brings Joyo Amazon's total fulfillment center capacity in China to over 75,000 square meters. The Beijing facility has modern logistics equipment and, together with the hardware and software that support it, provides Chinese customers a more enjoyable shopping experience. The Joyo Amazon headquarters and customer service center (which responds to emails and calls from Chinese customers) also are located in Beijing. Joyo Amazon is managed and staffed by Chinese nationals who best understand -- and who are focused on serving -- Chinese customers.

Our experience with China, including interactions with government licensing agencies, has been positive, and our biggest challenge has been to manage the high growth rate for Joyo Amazon. This is a great

P.O. BOX 81226, SEATTLE, WA 98108-1226
WWW.AMAZON.COM

Honorable Richard J. Durbin
February 18, 2010
Page 2

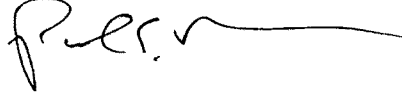
challenge to have, of course and, with investments such as in the Beijing fulfillment center, we look forward to meeting it on behalf of our customers.

Amazon has long been committed to protecting the privacy of customers. We know that customers care how information about them is used and shared, and we appreciate their trust that we will do so carefully and sensibly. We have supported important privacy legislation, such as Senator Feingold's bill for a Library, Bookseller, and Personal Records Privacy Act. We also are committed to free expression, and we are long-time supporters of the American Booksellers Foundation for Free Expression. In addition, Amazon has long been a leading proponent of maintaining the fundamental openness of the Internet and is a strong supporter of net neutrality.

Because Amazon's business in China does not include operating a network or Internet search engine, and because Joyo Amazon is run locally within China, we have not participated in the Global Network Initiative, which seems largely inapplicable to Amazon, and we did not know about or attend the open house last autumn. We are planning to stay abreast of developments in the GNI and, of course, we will keep focusing on customers, including their expectations for data privacy and security.

Thank you again for your letter and for the opportunity to respond.

Sincerely yours,

A handwritten signature in black ink, appearing to read "Paul Misener", with a long horizontal flourish extending to the right.

Paul Misener
Vice President, Global Public Policy



February 19, 2010

The Honorable Richard J. Durbin
Chairman
Subcommittee on Human Rights and the Law
United States Senate
Washington, DC 20510

Dear Chairman Durbin:

Thank you for your letter of January 29th following up on our correspondence last summer regarding how we address human rights issues in markets where we conduct business around the world. In keeping with Apple's letter of August 27th, 2009, let me again assure you that our company is committed to ensuring the highest standards of social responsibility wherever our products are made and sold, including in China.

Your letter asks if our business practices will change in light of reports of cyber attacks against U.S. government sites as well as U.S. companies including Google, which has suggested that it may change the way it runs its search engine in China. While Apple was not targeted by these attacks, we continue to be vigilant in protecting our internally housed data using Apple's industry-leading hardware and the robust security features of Mac OS X "Snow Leopard" Server software, which is constantly monitored by our global security team. With respect to questions concerning the filtering of customer searches in China, Apple is not in the search business and does not provide web services in China or host social networking sites there. Furthermore, Apple is neither a network operator nor an ISP, and has not been asked by the Chinese government for any customer information, or to filter customer inquiries and/or searches.

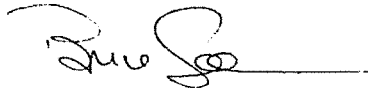
After two years in the device approval process, we began selling the iPhone in China in October 2009. We also began offering our Chinese customers direct access to the App Store, which sells more than 140,000 apps worldwide for use on the iPhone and iPod Touch. These applications – which are software products created and owned by independent developers who deliver them directly to customers' devices through the App Store – give Chinese consumers access to information, tools, educational materials, entertainment and games. The App Store is the largest of its kind in the world and has been a huge success not only in delighting customers, but also in providing local software developers and entrepreneurs an opportunity to write apps specifically for a particular country and/or region. We believe that the potential for the App Store in terms of its breadth of content and global reach is very significant, and we hope that its success will open more doors for equally transformative technologies in the future.

Apple appreciates your efforts to encourage companies to establish policies and procedures to address the potential for human rights violations, such as the principles established by networking companies in the Global Network Initiative (GNI). We see the GNI's voluntary objectives and principles as serving well certain networking segments of the technology

industry. Although Apple is not a networking company, we attended GNI's open house, and will continue to monitor the GNI's progress while remaining active in other industry efforts that more directly address the nature of our business. For example, we participate actively in the Electronic Industry Citizenship Coalition (EICC), a group of companies in the electronics industry that are working together to improve social responsibility in the global supply chain. Apple's Supplier Code of Conduct, which we described in detail in our August 27th letter, is modeled on and contains language from the EICC Code of Conduct, as well as from internationally recognized human rights conventions. In 2009, we significantly enhanced the scope of our supplier responsibility program, which we described in our August letter. Details of the expanded program will be in Apple's 2010 Progress Report on Supplier Responsibility, available soon at <http://www.apple.com/supplierresponsibility/>

In summary, Apple is proud to have established our own comprehensive and principled approach to human rights issues which we apply everywhere we conduct business around the world. We believe that there are many ways for companies to reach the goals of protecting individual freedom of expression and human rights and we believe our customers and employees are well served by the rigorous programs we have established within Apple.

Sincerely,

A handwritten signature in black ink, appearing to read "Bruce Sewell", followed by a horizontal line.

Bruce Sewell
Senior Vice President & General Counsel
Apple Inc.



Timothy P. McKone
Executive Vice President
Federal Relations

AT&T Services, Inc.
1133 23rd Street, NW
Suite 900
Washington, DC 20036

T: 202.453.4144
F: 202.453.4183
tm3703@att.com

February 18, 2010

Hon. Richard J. Durbin
United States Senate
309 Hart Senate Office Building
Washington, DC 20510

Dear Senator Durbin:

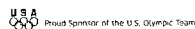
I am responding to your letter dated January 29, 2010, to our Chairman and CEO, Randall Stephenson.

AT&T shares your interest in recent events surrounding Google's business operations in China. As you know, AT&T operates one of the most extensive and sophisticated communications networks in the world, and we stand at the vanguard of efforts to protect our nation's communications capabilities from cyber-attack. As such, we treat as gravely important any cyber-attack of the magnitude reportedly suffered by Google, from whatever origin. We likewise appreciate your continued exploration of another challenge highlighted by Google's apparent decision to alter its policies for doing business in China, namely how best to advance the cause of human rights and the free flow of information in an increasingly interconnected world. Your leadership in this arena ensures that, in return for the clear benefits of globalization, our nation can still preserve and project its fundamental values. AT&T and its nearly 300,000 are committed to meeting the diverse needs of our employees, customers, suppliers, stockholders and business partners in all of the communities and nations where we do business, and we have established policies that promote human health and safety, ethical business behavior, personal privacy, and good stewardship of the environment.

AT&T has a global presence, which includes investing in subsea cable infrastructure, bilateral and roaming traffic exchange, and enterprise communications. Although AT&T does provide bilateral and roaming communications to and from China, within China AT&T is not a provider of mass market or consumer communications services, nor is it a licensed carrier that operates network infrastructure in the country. Rather, our emphasis in China is on our larger multinational business customers that are expanding their business presence in the country. We provide them advanced and reliable enterprise communications solutions, such as virtual private network capabilities. In doing so, AT&T's business in China at this time relies on commercial supply and correspondent relationships with Chinese carriers. Pursuant to cooperation agreements, these local carriers own and operate the necessary network equipment and communications infrastructure to support various business services, and they hold any necessary governmental licenses and related licensee obligations.¹

As we expressed in our prior letter to you of August 25, 2009, we are nonetheless mindful that government action can stifle freedom of expression. For this reason, we take quite

¹ AT&T has such relationships with, for example, China Telecom, China Unicorn and Unisiti, the latter of which is a joint venture in which AT&T owns a 25% minority interest.



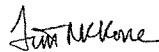
Senator Richard J. Durbin
February 18, 2010
Page 2

seriously our role in ensuring that government requests that could have the effect of limiting free speech or invading our customers' privacy undergo rigorous evaluation. At a minimum, when we receive a directive from a foreign government or agency to, for instance, block access to certain content or websites, we confirm that the request is authorized under local law; authenticate both that the request conforms with applicable rules and that the requesting person or institution is, indeed, authorized to submit the request; seek as much specificity as possible regarding the nature of the request; and, if the request is lawful and properly authorized, tailor our compliance with it as narrowly as possible. In the case of our operations in China, however, because our focus is on business customers, and the underlying communications infrastructure is provided by licensed Chinese carriers, to our knowledge AT&T has not been in direct receipt of any requests for assistance from Chinese law enforcement or other authorities.

Finally, AT&T did participate in the Global Network Initiative's Open House last year, and has participated in the follow-on workstream, which to date has included a series of GNI-led conference calls with industry participants and other stakeholders. We intend to continue to be a constructive participant in the workstream as it develops, and to otherwise continue our engagement with institutions determined to advance freedom of expression around the globe.

Thank you for seeking AT&T's perspectives on these critically important matters. Please feel free to contact me should you require additional information.

Respectfully,



Cc: Randall Stephenson
Tanya Acebedo
Charlene Richardson
Rodney A. Smith



Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Direct: 408 526 4000
FAX: 408 526 4100
www.cisco.com

February 19, 2010

The Honorable Richard Durbin
United States Senate
Washington, DC 20510

Dear Senator Durbin:

Thank you for your January 29th letter addressed to John Chambers regarding Global Internet freedom and China. I am responding to your questions in my capacity as Cisco's Chief Legal Officer.

Q1. Please provide a detailed description of your company's business in China.

A1. Our sales operations in China are as follows:

Cisco sells Internet Protocol-based networking and other products in China that enable data, voice, video and mobile communications. Our customers include enterprise businesses, telecommunications service providers, small businesses, universities, hospitals and other public institutions.

Our product offerings include network switches, which link networks of computers together, and routers, which direct the flow of packets of data between networks and across the Internet. Cisco also sells network management and security tools that allow customers to operate their networks without interruption 24 hours a day and to protect their networks from spam, malware, denial of service, and other malicious attacks or intrusions.

Cisco also sells a variety of other products, including "unified communications" products to link voice, video, data and mobile communications networks; IP phones; wireless network access points; cable access, set-top boxes and digital media products; videoconferencing and other on-line business collaboration technologies; and building management systems.

Cisco home networking products are available for purchase by consumers in China; they include voice and data modems, routers, video cameras, and other consumer devices.

All Cisco customers globally have access to Cisco training and support. In some cases we provide repairs and other technical support directly to customers; authorized resellers of our equipment may also provide support, and that is the

typical route for support internationally. 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.

Q2. What are your company's future plans for protecting human rights, including freedom of expression and privacy, in China? Please describe any specific measures you will take to ensure that your products and/or services do not facilitate human rights abuses by the Chinese government, including censoring the internet and monitoring political and religious dissidents.

A2. Cisco has adopted human rights guidelines to guide the conduct of our employees, and they are reflected in the Corporate Citizenship Report which we have shared with the Committee previously. As stated in our Report, 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."

As the Report notes, Cisco has adopted the following two principles from the UN Global Compact:

"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."

Cisco has also stated publicly that we don't customize or develop specialized or unique filtering capabilities to enable different political regimes to block access to information. We are comfortable that our activities in China conform to these principles.

While Cisco is not an Internet service provider like current Global Network Initiative (GNI) participants, we believe the GNI's core principles for network operation are appropriate for those companies that are network operators. Were Cisco to operate a network anywhere in the world, it would be our intention to act in accordance with those principles.

Q3. Did representatives of your company attend the GNI open house? If no, why not?

A3. Yes.

Q4. Does your company plan to participate in the GNI workstream? If no, why not?

A4. Cisco will continue to monitor progress on the GNI and remains willing to meet with the principals to discuss the group's goals and outcomes. However, the GNI model may not be suitable for computer hardware and network infrastructure suppliers since there are literally dozens of companies, both U.S. and non-U.S.-based, including some based in China, which sell equipment and software for operation of the Internet around the world.

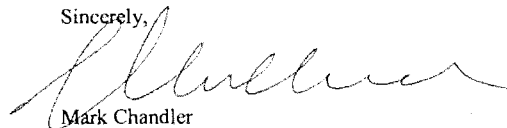
The most fundamental issue is how the purchasers and end users of information and communications technology in other countries are directed to use those products by their governments. This is beyond the control of hardware vendors whose product functionality is generic. In the case of Cisco, we sell equipment that meets global standards, and we believe our adherence to global standards plays a significant role in expanding access to information, undermining censorship and facilitating efforts to ensure the free flow of information. We consistently oppose efforts by foreign governments to enact and enforce local standards that would balkanize the Internet and undermine the free flow of information.

We believe these issues are more appropriately addressed by government efforts to drive consistency in global Internet standards and by industry associations, rather than by individual companies. This was illustrated last summer by the successful efforts of technology industry associations, governments and Internet users in China to oppose government efforts to mandate the installation of "Green Dam" filtering software on personal computers sold in China.

We do intend to continue discussions with other hardware and software technology companies on the development of best practices that prevent the balkanization of the Internet, support free flow of information globally, and maintain privacy protections for Internet users.

Thank you for the opportunity to respond to your questions on this important matter. Please let me know if I can provide any additional information.

Sincerely,



Mark Chandler
Senior Vice President and General Counsel
Cisco Systems, Inc.

*Dell Inc.
1225 I Street, NW, #300
Washington, DC 20005*

*Telephone: 202.408.3355
Telefax 202.408.7664
www.dell.com*



February 18, 2010

The Honorable Richard J. Durbin
U.S. Senate
309 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Durbin,

Thank you for your letter of January 29, 2010, which follows my August 27, 2009 letter to you and Senator Coburn. As the person responsible for Dell's corporate responsibility policies, I have again been asked to reply for the company. As I mentioned in my previous letter, Dell is committed to protecting human rights, whether with respect to our own employees, suppliers and their workers, or customers. As you have requested, this letter describes Dell's business in China, our plans for protecting human rights in China, and our engagement with the Global Network Initiative (GNI).

Dell's Business in China

Dell has been established in China since 1998. We assemble and sell a range of hardware products within China. These products include personal computers, printers, servers, storage devices and, most recently, smart phones. We also sell services and software to support these hardware products. Our hardware products allow our customers to access the media or content provided by other companies. Dell itself is not a media company or content provider. We are also not an internet service provider or a telecommunications service provider.

Dell's Commitment to Human Rights

Our employees. Dell is committed to treating our employees fairly and with dignity and respect. Our Code of Conduct sets out our commitment to workplace equality, compliance with all applicable legal requirements, and ensuring that our employees work in a safe and healthy environment.

Our supply chain. Dell has also taken steps to help ensure that working conditions in its supply chain are safe, that workers are treated with respect and dignity, and that business operations are environmentally responsible. Dell is a member of the Electronic Industry Citizenship Coalition (EICC), and we adhere to the Electronic Industry Code of Conduct. We are committed to working with socially responsible entities that comply with all applicable laws and regulations where they conduct their business, embrace high standards of ethical behavior, and treat their employees fairly, with dignity and respect. Both Dell and the EICC audit for adherence to applicable laws regulating wages, hours and working conditions. Dell requires its suppliers to adopt the EICC code of conduct. Suppliers must demonstrate a commitment to the health and safety of their employees and not use forced or indentured labor, or use raw materials or finished goods produced by forced or indentured labor.

Our customers. In addition, as I explained in my August letter, Dell is committed to protecting the privacy of our customers. Our privacy statement makes clear that Dell will only collect, store and use their personal information for limited business purposes and to support and enhance our relationships with them. We do not sell our customers' personal information. We expect our employees to appropriately safeguard our customers' information and comply with Dell's privacy policies and applicable laws on customer privacy.

Our Approach to Protecting Human Rights When Faced With Government Mandates in China or Elsewhere. Access to technology and the Internet is critical in promoting human rights and freedom of expression around the world. Dell is proud of our role in placing this powerful tool in the hands of our global customers. We recognize, however, that issues may arise with respect to government mandates that may impact customers in a particular country.

When facing specific government mandates where citizens' freedom of expression or privacy may be impacted through the use of a Dell product, we look to our own Code of Conduct as well as applicable best practices. In this regard, Dell is familiar with the GNI principles and guidance, which generally mirror our approach.

We recognize that issues involving governmental policies can have larger implications that are beyond any one company's ability to deal with effectively, and so we attempt to address such mandates by working with other companies that may be similarly affected using our trade associations, and by engaging with governments through our associations to express the concerns of our industry.

We strive to provide customer choice when at all possible, consistent with local law. If not possible, then we seek to avoid or minimize the impact of government mandates or restrictions on freedom of expression and privacy. We also seek to give clear, prominent, and timely notice to customers when a specific government mandate on hardware vendors may impact their ability to fully use our products.

The Global Network Initiative

In my August letter to you, I noted that Dell recognizes the value of industry best practices, and that we were open to discussing the value of GNI membership as well as other options specifically tailored to the IT hardware sector. Following my letter, Dell attended the GNI "Open House" on September 10, 2009. We found this informational session instructive and informative. Having participated in this dialogue and reviewed GNI's principles and workstream, we applaud the GNI's efforts to develop guiding principles and best practices, and to increase transparency. We are supportive of these efforts. We believe that the GNI's work is applicable to media and content companies, who are frequently and consistently faced with government mandates to censor or monitor content. Dell does not fall into this category, given our company focus on selling hardware. As a result, we declined the invitation to join the ongoing workstream.

We continue to believe that the hardware industry requires an approach more tailored to our own circumstances. We are working with industry partners and stakeholders to develop a list of principles in collaboration with interested stakeholders designed to meet the specific needs and issues faced by the hardware industry.

Again, we appreciate your work to protect human rights around the world. Dell is committed to protecting human rights, whether with respect to our own employees, our suppliers and their workers, or customers.

Sincerely,



Gilbert F. Casellas
Vice President
Corporate Responsibility
Dell Inc.

February 18, 2010

The Honorable Richard Durbin
Chairman
Subcommittee on Human Rights and the Law
United States Senate
Washington, DC 20510

Dear Senator Durbin:

Thank you for your letter dated January 29th regarding the announcement from Google regarding a cyberattack that they traced to sources in China, as well as the Chinese government policies that Google agreed to comply with as part of their search engine business operations in China. I would note that eBay was not impacted by the reported cyberattack episode.

eBay Inc. is a global ecommerce and payments business that helps connect buyers and sellers globally through the Internet, empowering individuals, entrepreneurs and small business retailers in the global marketplace. The Chinese people play a large and growing role in the global economy and eBay has worked to best serve our Chinese customers for a number of years. Engaging with partners and adapting our strategies to meet evolving challenges, eBay continues to work to serve well Chinese entrepreneurs and consumers on the Internet, as we do for entrepreneurs and consumers around the world. Currently, eBay Inc. does not have a marketplace business in China to serve the Chinese domestic market. Instead, eBay is a minority stakeholder in Eachnet, a Chinese-based joint venture conducting a domestic Internet marketplace business that serves Chinese Internet users.

Aside from our minority investment in Eachnet, eBay does have a handful of other operations in China at this time. eBay directly supports "cross border trade" by Chinese sellers who use the Internet to reach customers outside of China. We similarly serve a number of entrepreneurial sellers in other Asian countries and regions, including Japan, Taiwan and Southeast Asia. eBay has facilities in Shanghai and Beijing that promote the cross border trade business. In addition, eBay engages in some regional customer service and some development work and technical operations from China. Finally, we believe that expanding the availability of our payments services to Chinese entrepreneurs will promote ecommerce and better serve Chinese users, and our payments business, PayPal, is currently seeking a Payment Service Organization license in China.

As I related to you in my September letter, eBay Inc.'s initial experience with the Global Network Initiative "GNI" was through Skype, the Internet communications business that was then a part of eBay Inc. In the ensuing months, eBay Inc. completed the sale of a majority stake in Skype, which now operates as a stand-alone business, and I understand that Skype continues to be engaged in discussions with the GNI.

eBay believes that the moral, legal and regulatory matters you have identified through your efforts should be of great importance to all globally engaged companies. An eBay representative did attend the GNI "Open House" held in the fall. From the specific perspective of eBay's payments and marketplaces businesses, few if any of the issues currently being addressed by the GNI appear to be

directly applicable. However, eBay has continued to monitor the development of the GNI effort related to expansion beyond the initial Internet search and communications companies:

I hope this information is helpful to you as you continue to review the role that information technology, the Internet, and rapidly evolving digital communications play in the world.

Regards,

John Donahoe
President and CEO

February 19, 2010

The Honorable Richard Durbin
U.S. Senate Committee on the Judiciary
Subcommittee on Human Rights & the Law
United State Senate
Washington, D.C. 20510

Dear Chairman Durbin,

Thank you for your letter of January 29, 2010 to Facebook, Inc. ("Facebook" or "the company") regarding the company's potential participation in your forthcoming Subcommittee hearing on internet freedom in China. Facebook does not have any business operations or significant user footprint in China and will therefore respectfully decline to participate in the March hearing. We are nonetheless pleased to provide you with the following response regarding our business practices and policy views on the important issues you have asked us to address. As you know, this letter is an addition to our prior response to your August 6, 2009 letter.

Facebook's mission is to give people the power to share and make the world more open and connected. At the same time, we recognize that social norms around information sharing, connection, openness and privacy vary from country to country and culture to culture. As our business grows internationally, we work hard to offer tools and services that empower users while recognizing the importance of respecting local conditions, traditions and legal requirements.

As a relatively young company, we are learning about how to accomplish both goals simultaneously. We are carefully watching the experience of similarly situated, but longer-tenured companies and trying to learn from their experiences. We have met with human rights experts at various Non-Governmental Organizations ("NGOs") and have an open door and an open mind to hear their concerns. We look to the Global Network Initiative ("GNI") as a benchmark to which we compare our own efforts. Further, we are also always open to constructive collaboration with other companies, federal agencies, NGOs and other experts.

Facebook's Commitment to Human Rights

We hope that the Facebook service advances human rights everywhere by providing people around the world with access to free, fast, simple, multi-lingual communications tools. Facebook provides a platform for user generated content. Providing the ability to communicate and share protects and advances human rights because people can witness



and report on their world in real time. In a very real sense, Facebook users can be journalists by reporting on the world they experience.

We have instituted certain rules, enshrined in our Statement of Rights and Responsibilities to facilitate the sharing of content that is appropriate to share on Facebook. These rules make sure that when sharing an opinion turns into direct statements of hate or threats against an individual, for example, or when users upload nudity, pornography, or violent photos or videos, the professional reviewers on our team take quick action to respond to reports, remove the content, and either warn the sender or disable the accounts of those responsible. It is only after content is shared that if other users believe that content violates our Terms of Service, they can report the potentially offending content for us to investigate. When content reported to us – shared from anywhere in the world – violates our Terms of Service, or when content shared from a particular jurisdiction violates that jurisdiction's local laws or customs, Facebook may take down that content.

Facebook Does Not Have a Business Presence in China

To respond to your more specific questions, put simply, Facebook has no business operations in China or, for that matter, in most countries of the world. More explicitly, we do not employ any staff in China. We do not have any offices in China. We do not store any user data in China, nor do we have individuals selling ads in China. Although, undoubtedly some Facebook users reside in China and some users who are in China occasionally may access Facebook, Facebook has not been widely accessible to users in China since June 2009.

Further, we do not have any present plans to open an office in China, and no plans to make any changes to the Facebook service for users in China. Facebook also does not store any user data outside of the United States.

Facebook's Engagement with the Global Network Initiative

Although our policy team is small in staff numbers, we did participate in a GNI open house. Based on what we have learned, we do not anticipate more expansive engagement in the GNI unless and until the growth of our international business operations warrants it and we have the staff hours to dedicate to participating properly. While not being formal participants at this stage, we nevertheless hope to stay informed about the work of the GNI and use it to inform and further shape our decisions with respect to our company growth worldwide and development and implementation of our policies.

* * * * *

Facebook appreciates the opportunity to respond to your questions, as well as your continued attention to and leadership with respect to this issue. Should the facts about our business change as our business grows internationally, we would welcome the opportunity to testify at a subsequent hearing and we will continue to meet with your staff in the

The Facebook logo, consisting of the word "facebook" in a white, lowercase, sans-serif font on a dark, textured rectangular background.

13

interim. If we can be of further assistance to you or your staff, please feel free to contact me at any time.

Sincerely,

Timothy Sparapani
Director, Public Policy
Facebook



Fortinet Confidential; By Facsimile and Email

February 19, 2010

U.S. Senator Richard J. Durbin
 United States Senate
 Washington D.C. 20510
 Facsimile: c/o Heloisa Helena Griggs at 202-228-0781
 Email: c/o Lauren Myerscough-Mueller at Lauren_Myerscough-Mueller@Judiciary-dem.senate.gov

Dear Senator Durbin:

Thank you for your letter dated January 29, 2010. In terms of a description of our business, Fortinet sells network security appliances principally designed to help protect the privacy and data of individuals and businesses from computer hackers and other threats. We are a relatively small and young company – we remain less than 1/100th the size of Cisco, for example, and we have been selling product only for the past 8 years. Our overall revenues were approximately \$250 million in 2009, and, during 2009, our sales to China were approximately 3% of our overall sales. Our sales to the Chinese government were only a fraction of this already small amount, and our channel partners are required to abide by U.S. export laws for all sales. Our products are used to provide a broad array of network security. Some fraction of our products sold are used for web-content filtering. For web-content filtering, we provide customers certain categories designed to allow customers to filter out categories such as violence, child abuse and pornography, and other categories where there is a legitimate public interest in filtering the content.

Despite the fact we are a relatively small and young company, through our trade compliance team and processes, in accordance with the U.S Export Administration Regulations, we spend considerable effort and money to screen, export license or prohibit sales into certain countries, which are also often countries that may have poor human rights records. We are very proud of the processes we have established in this regards, and we intend to continue to ensure we have proper resources and processes and to continue to evolve and improve these functions. In addition to meeting legal requirements, as a matter of company policy, we have prohibited sales into certain countries with poor human rights records even when such sales are in fact permissible under U.S. laws.

In line with continuing to consider ways to improve, we have attended GNI events and talked with GNI representatives to learn about the organization's objectives and to further assess the degree to which our involvement with the GNI will have a real impact in furthering human rights. We did attend, and enjoyed participating in, the GNI open house on September 10, 2009, and have attended subsequent calls, and we are participating in upcoming events. We are still in the assessment phase as to whether our joining the GNI would have any meaningful positive impact

Fortinet, Inc.
 1090 Kifer Road | Sunnyvale, CA 94086 | USA
 Main: (408) 235-7700 Fax: (408) 235-7737



on human rights. We may join the GNI in the future and we intend to continue to assess the GNI and whether our joining this organization would have a meaningful positive impact, and we welcome any suggestions you may have as to actions we can take to improve human rights.

Thank you again for your letter and time on this matter.

Sincerely,

FORTINET, INC.

A handwritten signature in black ink, appearing to read "John Whittle".

John Whittle
Vice President, General Counsel

cc: Ken Xie, CEO, Fortinet, Inc.
Renee Roe, Global Trade Compliance Officer, Fortinet

Fortinet, Inc.
1090 Kifer Road | Sunnyvale, CA 94086 | USA
Main: (408) 235-7700 Fax: (408) 235-7737



Hewlett-Packard Company
1331 Pennsylvania Ave NW
Suite 1300 North
Washington, DC 20004
www.hp.com

Larry Irving
Vice President
Global Government Affairs

(202) 637-6751 Tel
(202) 637-4974 Fax
larry.irving@hp.com

February 19, 2010

The Honorable Richard J. Durbin
United States Senate
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Durbin:

Thank you for your letter of January 29, 2010, regarding Hewlett-Packard's approach to human rights issues in China and the Global Network Initiative (GNI). As always, we welcome open and constructive dialogue about our corporate social responsibilities and commitment to promoting human rights.

HP is committed to operating ethically as a company and respecting human rights in our conduct globally, including in China. We pursue this commitment through rigorous internal corporate policies and procedures as well as through engagement with outside stakeholders, other businesses, and institutions. And we subject ourselves to internal and third-party assessments and evaluations of our performance. These policies and engagement apply in full to our operations in China; HP operates around the world, including in China, under one, high-level code of conduct and set of policies.

In terms of internal policies and procedures, HP has integrated human rights principles into business decision-making. HP has adopted a Global Citizenship Policy, under which all employees worldwide must uphold the human rights articulated in the Universal Declaration of Human Rights, which includes the freedom of expression and the right to hold opinions without interference. All employees must commit to HP's Standards of Business Conduct, including to support and respect the protection of human rights. HP's Global Master Privacy Policy and Online Privacy Statement protect personal information worldwide against unauthorized use or disclosure. Finally, HP's Human Rights & Labor Policy embeds international human rights standards in HP's global personnel policies and guidelines.



Hewlett-Packard Company
1331 Pennsylvania Ave NW
Suite 1300 North
Washington, DC 20004
www.hp.com

We also seek to impose human rights and other global citizenship standards where we can in our supply chain, even though we lack operational control. HP's Supplier Code of Conduct promotes responsible practices in labor, human rights, ethics, the environment, and worker health and safety at our suppliers. Our supply chain program promotes respect for the human rights and labor conditions of more than 340,000 workers worldwide. In 2008, HP audited 129 supplier sites for compliance with this code of conduct, bringing our total since 2005 to 480.

To maximize enforcement of HP policies, we provide multiple anonymous channels for employees to report any noncompliance or ethical concerns. Our Chief Ethics and Compliance Officer oversees these mechanisms, processes all reports, and reports independently to the Audit Committee of the Board of Directors.

HP's staunch commitment to human rights is also reflected in our corporate governance structure. Our Global Citizenship Council, which comprises senior executives, meets regularly to coordinate HP's global citizenship strategy across the company. Our global citizenship framework consists of five core areas: ethics and compliance, environmental sustainability, human rights and labor practices, privacy, and social investment. The Council advises HP's Executive Council—a body that includes HP's Chief Executive Officer and the heads of each HP business unit—which retains overall responsibility for global citizenship as part of our business strategy. The Executive Council, in turn, reports directly to the Board of Directors.

HP also convenes a Privacy and Data Protection Board, which provides company-wide oversight for privacy and data protection. Board members are from the Privacy, Legal, Information Technology, Security, Internal Audit, Internet, Human Resources, and Government Affairs functions, as well as from each business unit and region. At quarterly meetings, board members discuss high-level priorities, assess programs, launch projects, make strategic decisions and resolve any issues escalated to this level. External experts are regularly invited to discuss privacy trends and developments. Members work throughout the year on sub-teams that handle specific privacy issues in the company.



Hewlett-Packard Company
1331 Pennsylvania Ave NW
Suite 1300 North
Washington, DC 20004
www.hp.com

In terms of external engagement, we pursue our commitment to human rights and more broadly global citizenship—in China and worldwide—by collaborating with multiple stakeholders, other businesses, and institutions, including targeted initiatives specific to our business.

We have been a member since 2002 of the UN Global Compact, which sets forth ten universally accepted principles to which participating companies must try to align their business operations and strategies. The UN Global Compact is based on the principles of the Universal Declaration of Human Rights, which is the foundation of the international human rights system and protects freedom of expression and privacy. As a member of the UN Global Compact, HP's commitment extends to Principles 1 and 2, which state: "Businesses should support and respect the protection of internationally proclaimed human rights; and make sure that they are not complicit in human rights abuses."

HP played a key role in the Business Leaders Initiative on Human Rights, a group of 16 global companies that developed a step-by-step guide for businesses to integrate Universal Declaration of Human Rights principles (again, which include the freedom of expression and privacy) into their management decision processes. This guide was developed in cooperation with Realizing Rights: The Ethical Globalization Initiative and the UN Office of the High Commissioner for Human Rights and includes a Business and Human Rights Matrix, which helps companies conduct self-assessments and identify any gaps between their policies and international human rights standards. Former UN High Commissioner on Human Rights Mary Robinson chaired this effort.

With respect to respect for human rights in the supply chain, HP helped develop and abides by the Electronic Industry Code of Conduct, which outlines standards to ensure that working conditions in the electronics industry supply chain are safe, that workers are treated with respect and dignity, and that manufacturing processes are environmentally responsible. This code of conduct was developed under the auspices of the Electronic Industry Citizenship Coalition, which HP helped found in 2003.



Hewlett-Packard Company
1331 Pennsylvania Ave NW
Suite 1300 North
Washington, DC 20004
www.hp.com

We also engage actively on privacy issues with regulators, non-governmental organizations (NGOs), and other businesses globally and on a regional basis, including in Asia. For instance, under the auspices of the Asia-Pacific Economic Cooperation (APEC) forum, stakeholders have been working to develop cross-border data privacy rules. Following an invitation from the Department of Commerce and the Federal Trade Commission, in 2008 HP joined the APEC Privacy sub-group to help develop these rules.

In terms of transparency and accountability, we are committed to transparency to allow inside and outside actors to credibly assess and evaluate HP's human rights performance. Pursuant to the UN Global Compact's reporting requirements, HP publishes an annual public Global Citizenship Report, which the UN Global Compact Office has officially recognized for its high quality and comprehensiveness. The report provides detailed reporting on HP's ethics and compliance program, our ongoing privacy initiatives, and our human rights practices.

HP has invited outside stakeholders to help assess our performance and provide guidance going forward. For instance, in 2007, we established the Stakeholder Advisory Council (SAC), which was comprised of five prominent NGO representatives as well as senior HP executives. The SAC met regularly, and the NGO members helped us identify and prepare for potential business risks and provided advice on our leadership strategy for our global citizenship initiatives. In late 2008, HP expanded and renamed SAC as the Trusted Advisory Network (TAN). And, as noted, HP provides internal mechanisms to ensure accountability such as channels for whistleblowers to report any noncompliance or ethical concerns.

HP has consistently earned good marks from NGOs and others for our actions and policies. Students and Scholars Against Corporate Misbehavior (SACOM), a Hong Kong-based NGO that monitors corporate behavior and advocates for workers' rights, wrote in a 2008 report that "Hewlett Packard is setting the pace for social responsibility in China." Corporate Responsibility Officer (CRO) ranked HP number 5 on CRO's 100 Best Corporate Citizens for 2009. On the rare occasion when the human rights community has criticized HP, we have been very responsive. For example, CSR Asia—a consultancy focused on



Hewlett-Packard Company
 1331 Pennsylvania Ave NW
 Suite 1300 North
 Washington, DC 20004
www.hp.com

sustainable business practices in Asia—last year commended HP for our responsiveness to a report that was critical of our supplier factories' working conditions.

Through the range of measures described above—internal policies and procedures, external engagement, and transparency and accountability—HP seeks to ensure that we honor human rights in all of our activities, in China and everywhere else we do business.

HP operates around the world, and has major product development and manufacturing operations throughout the United States, as well as in China, India, Ireland, Israel, Japan, The Netherlands, Puerto Rico, Russia, Singapore, and the United Kingdom. HP has maintained a presence in China since 1981. We are the second largest PC vendor in China and also sell printers, servers, workstations, and other HP products, as well as providing enterprise services to that market. HP does business in more than 680 cities in China, and nearly 7,000 Chinese retail stores carry HP products.

HP has manufacturing facilities in China. In Shanghai, we produce desktop PCs, servers, and printers. In Chongqing, we have recently begun production of desktop and notebook PCs. In addition, many of our products are manufactured by "Original Design Manufacturers" in China under contract manufacturing arrangements.

Besides our sales and manufacturing activities, HP conducts research and development in China, including through an HP Labs facility in Beijing and the China Design Center in Shanghai. HP Labs is the exploratory and advanced research group for HP, while the China Design Center focuses on creating products for the China market as part of HP's "Designed in Asia, for Asia" program.

In November, HP and 3Com Corporation announced that they had entered into a definitive agreement under which HP will purchase 3Com, which also has operations in China. That acquisition is subject to customary closing conditions, including the receipt of regulatory approvals.

* * * * *



Hewlett-Packard Company
1331 Pennsylvania Ave NW
Suite 1300 North
Washington, DC 20004
www.hp.com

With respect to your questions on GNI, representatives of HP attended the GNI open house in September 2009. We were represented by our Chief Privacy Officer and our Social Responsibility Program Director, both of whom attended the meeting in San Francisco, and HP's Congressional and Federal Affairs Executive Director, who attended the meeting in Washington, DC.

We have indicated to GNI that we would be interested to learn more about the results of their workstreams; but, rather than participate actively, we intend to continue to focus our people and resources on the initiatives in which HP is already involved that are tailored to the needs of our particular business. We have devoted significant resources to other initiatives and efforts and pursued them with a long-term approach that involves integrating human rights considerations into our business practices. These efforts are multi-year commitments, and HP continues to leverage its past efforts and build upon the foundation that it has collaboratively laid with multiple stakeholders.

When we consider participating in any new initiative, such as GNI, we consider a variety of factors, including: whether participation in the initiative would dilute our ongoing human rights efforts or detract from our sustained focus on areas where we are already committed; whether it is an initiative where we can add maximum value, given the nature of our business and the challenges germane to it; and whether the initiative would be duplicative of existing efforts. We believe our current work in the area of global citizenship is robust, adaptable to emerging issues, and tailored to maximize our impact given the sectors in which we operate. As indicated, however, HP is open to continuing to learn more about GNI.

I look forward to our continued work with you on these and other important issues.

Very truly yours,

A handwritten signature in black ink that reads "Larry King".



*Office of the Vice President
Governmental Programs*

*1301 K Street Northwest, Suite 1200
Washington, DC 20005 3307*

February 19, 2010

The Honorable Richard J. Durbin
Hart Senate Office Building, Room 309
United States Senate
Washington, DC 20510

Dear Senator Durbin:

I am pleased to respond on behalf of IBM to your letter to our Chairman and CEO, Sam Palmisano, dated January 29, 2010. We appreciate this opportunity to describe IBM's business in China and our company's policies and practices with regard to Internet freedom.

IBM operates in more than 170 countries with approximately 400,000 employees worldwide, with our non-U.S. operations generating more than 60 percent of IBM's revenue in 2009. IBM's business is focused on serving large enterprise clients with a full range of information technology solutions – we do not provide Internet, telecommunications, or content services to individual consumers.

In recent years, IBM has transformed itself into a globally integrated enterprise, which has improved overall productivity and is driving investment and participation in the world's fastest growing markets, including China. IBM has operated in China for decades. We now have offices in 26 cities throughout China and generated 10% revenue growth in China in 2009. IBM conducts sales, research, development, manufacturing and service delivery operations in China. Our business is principally focused on supporting the IT needs of large enterprise customers in China in industries such as financial services, transportation, retail distribution, and health care. IBM has also located the headquarters for our Growth Markets Unit in Shanghai, from where we manage IBM's business in our fastest growing emerging markets around the world.

The fundamental principles underlying the codes of conduct outlined by many corporate responsibility and citizenship initiatives, including the Global Network Initiative (GNI), are ones that IBM has been successfully addressing for decades through its own internal principles, global policies and management system. As a global business leader, IBM believes that world trade and investment is a force for positive change in all areas of business and society. For nearly a century, IBM has pioneered global commerce while also providing business leadership in such vital areas as equal opportunity, diversity, respect for the environment, supply chain standards, ethical behavior, and in services to communities worldwide. IBM applies its high global standards in China as well as in every other country in which the company operates.

At IBM, we have long understood that business success is linked to the overall interests of the public and society. This understanding was perhaps best articulated by former IBM CEO Thomas J. Watson, Jr., who wrote in 1969: "We accept our responsibilities as a corporate citizen

in community, national and world affairs; we serve our interests best when we serve the public interest. ... We acknowledge our obligation as a business institution to help improve the quality of the society we are part of. We want to be in the forefront of those companies which are working to make our world a better place."

Underpinning IBM's values is our company code of ethics, the IBM Business Conduct Guidelines. IBM requires all employees to certify annually that they have read and understood IBM's Business Conduct Guidelines, which specify IBM's standards of business ethics, basic values, and principles.

In our annual Corporate Responsibility Report, we publish our performance against those goals, and we report using the Global Reporting Initiative standard at the "A" reporting level. More information about IBM's corporate policies in the areas of corporate responsibility and our annual report may be found at our website: <http://www.ibm.com/ibm/responsibility/>.

On a global basis, IBM has received numerous awards for corporate social responsibility, including awards for specific areas of CSR such as environmental performance, workplace best practices, and community programs, as well as awards recognizing our overall CSR performance. For example, IBM was ranked third overall in the 2009 Corporate Responsibility Officer ranking of top corporate citizens in the United States, and the company was ranked as the number one ethical corporation by Covalence, the Swiss ethical ranking agency.

Because IBM follows the same high ethical standards and takes a strong interest in social responsibility wherever we operate, IBM has also been recognized in China with many awards for corporate citizenship, including: Five Star Outstanding Corporate Citizen in China, Most Responsible Multinational Corporation in China, Outstanding Contribution to Social Responsibility and Most Respected Company.

The company believes it can most effectively continue to achieve the highest levels of corporate conduct through adherence to the corporate policies and directives that govern IBM's operations worldwide. IBM will continue to monitor the many new codes and principles as they relate to this issue and will, when appropriate, update its own corporate policies and directives to maintain the company's objectives. Although the Global Network Initiative is principally concerned with consumer Internet services that IBM does not provide, we will continue to monitor it and other industry efforts as we keep our own corporate policies up to date.

Thank you for this opportunity to inform you about IBM's business in China and our strong programs in corporate social responsibility.

Sincerely,



Christopher A. Padilla
Vice President, Governmental Programs

1333 New Hampshire Ave., NW
Washington, DC 20036

Direct Dial: 202-419-3580
Email: radams@lenovo.com

VIA EXPRESS MAIL AND EMAIL

February 19, 2010

The Honorable Richard J. Durbin
United States Senate
309 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Durbin:

Thank you for your letter dated January 29, 2010, regarding the Global Network Initiative (GNI) and the Internet. We appreciate the opportunity to respond and to tell you more about our company.

Lenovo is a global corporation with operations in over 60 countries. Lenovo is one of the leading producers of personal computers and servers in the world. Lenovo does not produce Internet connection hardware, nor does it provide Internet connection or network services. Lenovo stock is publicly traded on the Hong Kong Stock Exchange, and the company is led by an international management team and board of directors. Lenovo's US Executive Headquarters are located in Raleigh, North Carolina. Lenovo maintains its Principal Operations in Raleigh, North Carolina; Beijing, China; and Singapore. The company has Research Centers in each of those three locations, and in other cities in China and Japan. Lenovo Sales Headquarters are located in New York, New York; Paris, France; Beijing, China; and Sydney, Australia.

Lenovo has an extensive record of corporate social responsibility. Indeed, we are committed to taking care of the long-term economic, social, and environmental health of our company and the communities in which we operate. Lenovo ranks among industry leaders in the promotion of green technologies, the development of energy efficient products, and the implementation of environmental best practices. The company dedicates a portion of its revenues each year to social programs. Most recently, Lenovo provided equipment and financial assistance to the American Red Cross for recovery efforts in Haiti.

Lenovo is committed to protecting human rights. We are a member of the United Nations Global Compact, which is a public-private strategic policy initiative for businesses committed to aligning operations and strategies with ten universally accepted principals

Page 2

in the areas of human rights, labor, the environment, and anti-corruption. As a signatory, we "support and respect the protection of internationally proclaimed human rights" and ensure that our business practices "are not complicit in human rights abuses." Numerous U.S. information technology companies and non-profit organizations, including participants in GNI, are also signatories to the Global Compact. The United Nations Special Representative on Business and Human Rights has observer status in GNI.

Moreover, Lenovo is a member of the Electronics Industry Citizenship Coalition (EICC) and an adherent to the EICC Code of Conduct for the Global Electronics Supply Chain, which safeguards the working and environmental conditions of our employees and those of our suppliers, including in the area of human rights. To that end, Lenovo has established strong EICC compliant operations and conducts independent third-party EICC audits. During recent audits at our facilities in China and India, Lenovo received a compliance score of greater than 90 percent across environmental, labor, ethics, and management practices. Similarly, as of April 1, 2009, nearly 95 percent of Lenovo's tier-one suppliers have signed on to and abide by the EICC reporting and compliance requirements and submit to third-party independent audits. As is the case with the Global Compact, numerous U.S. information technology companies, including participants in GNI, are also members of the EICC.

As a publicly traded corporation, our shareholders, employees, and customers expect us to operate in a socially responsible, legal, and transparent manner. With regard to GNI, Lenovo had not considered participating because we are not an Internet hardware manufacturer, nor an Internet service provider or network manager. However, we continue to learn about and study it. As previously discussed, Lenovo is an active participant in other important international initiatives that share many of the same goals as GNI. Lenovo has taken significant steps to protect the rights of our workers and customers throughout the world. As a company dedicated to these values, we are consistently evaluating ways to improve our business, while positively contributing to the development of the communities in which we operate.

Again, thank you for the opportunity to respond.

Sincerely,

A handwritten signature in black ink, appearing to read 'Rachel A. Adams', written over a horizontal line.

Rachel A. Adams
Vice President and Assistant General
Counsel



February 15, 2010

The Honorable Richard J. Durbin
The Honorable Tom Coburn
United States Senate
Washington, DC 20510

Dear Chairman Durbin and Ranking Member Coburn:

Thank you for your follow-up letter of January 29 to Greg Brown regarding Internet freedom and the Global Network Initiative (GNI). We share your interest and concern regarding the recent cyber-attacks and broader questions regarding Internet security, privacy, and the responsibilities of Information and Communications Technology (ICT) firms operating in the United States and markets around the world.

Undoubtedly, ICT products provide the means to revolutionize the ability of people, enterprises, and governments – around the world – to communicate and cooperate. Yet technology solutions are implemented within a framework of laws and regulations; the communications sector remains highly regulated through a web of operating licenses, frequency spectrum allocations, equipment type approvals, and network access licenses for communications equipment. Content restrictions exist in many markets – sometimes in the name of protecting domestic culture or morals, and sometimes for explicit political reasons.

Motorola's experience, in over 20 years of successful operations in China is to de-emphasize the political aspect of telecom policies, and promote technology neutral policies in the areas of technical standards, licensing, type approvals, etc. While not always successful, it has proven to be an effective means to stimulate innovation, and the development of the communication industry and services in China.

As we stated in our August 21 letter, Motorola is a strong proponent of protecting human rights, as expressed in the Motorola Human Rights policy (www.motorola.com/humanrightspolicy). We require every employee to abide by an ethical code of conduct as detailed in our Code of Business Conduct (www.motorola.com/code); the management of health, environment, and safety guidelines (www.motorola.com/ehspolicy); and our supply chain partners to abide by our Supplier Code of Conduct (www.motorola.com/suppliers/code).

Motorola established a representative office in China in 1987. Today Motorola has one holding company, five wholly-owned subsidiaries, five joint ventures, and 23 branch offices across China. Our head count number is about 8,000 employees. Operations range from sourcing, research and development; manufacturing, sales, and service.

Our largest customers in China are cellular operators that provide mobile communications and Internet access to nearly 700 million Chinese citizens per year. We serve government and enterprise customers with a range of mobile communications products and services.

We understand you strongly support the Global Network Initiative (GNI) to identify business practices and principles to guide operations in markets where government laws and practices may compromise the free flow of information and individual privacy. Motorola is a company with an 80-year history of innovation.

Motorola, Inc., Corporate Offices
1303 E. Algonquin Road, Schaumburg, IL 60196 U.S.A. Tel: +1 847 576 0770



in communications, with operations in over 70 countries and we are acutely aware of our responsibility to operate ethically in all aspects of our business.

Motorola works to support the principles promoted by the GNI.

- We strive to promote the freedom of expression - the bedrock objective of our entire solutions portfolio. Our devices, infrastructure equipment, and services are focused on expanding the means for people and enterprises to communicate through voice, data, and video transmissions.
- Privacy is another core value and product area. People have the right to control their personal information, and determine how it is collected and used. We are committed to protecting the privacy of those who submit personal information to Motorola. We train our employees on our privacy policies and practices, and we provide additional support for people whose jobs involve handling personal information. We work closely with third parties handling personal information on our behalf to ensure that the highest privacy standards are maintained. Employees who violate our information protection policies are subject to disciplinary action, including dismissal. Agents and subcontractors face contractual penalties or termination.
- We build technologies into our products to allow our customers to better protect their personally identifiable and confidential information. Our products are designed to protect the users' privacy and security. We include technology to guard against external interference and provide voice data encryption on mobile phone networks. Our mobile phone user manuals provide information about privacy and security risks, highlighting privacy- and security-protection functions.

We have internal processes in place to enable responsible company decision making to ensure – from the board of directors on down – the implications of our business operations in China on these core values. We believe associations such as the GNI, may serve a useful role to assist companies to address the challenges of navigating between ethical principles and local laws and regulations. However, our general practice is not to sign external ethics codes and standards. Such proliferation of external standards makes commitment to all of them unfeasible. Thus far we remain convinced that our internal program is best for all our many stakeholders.

Moving forward, we have designated Mrs. Yardly Pollas-Kimble, Sr. Director of Congressional Affairs for Motorola, to serve as our point of contact if your office would like to further engage on this issue and GNI. She can be contacted at 202-371-6903, as we would be happy to participate in future GNI Open House events.

Thank you for reaching out to Motorola on this important issue. I'm happy to discuss this further with you as the issues evolve and appreciate your support and attention.

Sincerely,

Karen P. Tandy
Senior Vice President
Public Affairs and Communications

Motorola, Inc., Corporate Offices
1303 E. Algonquin Road, Schaumburg, IL 60196 U.S.A. Tel: +1 847 576 0770



1211 AVENUE OF THE AMERICAS • NEW YORK, NY 10036 • 212-852-7100 • FAX: 212-852-7094

RUPERT MURDOCH, A.C.
CHAIRMAN AND CHIEF EXECUTIVE OFFICER

February 18, 2010

The Honorable Richard J. Durbin
Chairman
Human Rights and the Law Subcommittee
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Durbin,

Thank you for your letter dated January 29, 2010 informing me of the impending hearing of the Human Rights and the Law Subcommittee on "Global Internet Freedom: Corporate Responsibility and the Rule of Law." I would like to stress that the free flow of information and freedom of expression are fundamental to News Corporation's business as a global media and entertainment company. We also recognize the importance of respecting the privacy of our customers and users. We therefore welcome your attention to these critical issues.

I think the answers to the questions posed in your letter are again best answered by a description of MySpace, Inc.'s business arrangements in China, its global approach to content and its cooperation with law enforcement.

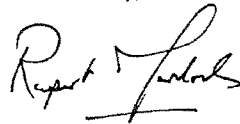
As described in my letter to you dated August 27, 2009, MySpace, Inc. licensed its brand and technology to a social networking site in China formerly known as MySpace.cn. This locally owned, operated and managed company continues to be responsible for compliance with Chinese law. MySpace.cn's users are informed at the time of registration that the site is subject to Chinese law.

MySpace, Inc. also operates MySpace.com, the U.S.-based English language site that is globally available to all Internet users. MySpace.com user data and content are hosted in California and the site is governed by U.S. law. MySpace.com does not filter or block any content in order to comply with foreign laws that relate to content restrictions and does not intend to do so in the future. Rather, MySpace.com enforces the content rules contained in the Terms of Use that are posted on every page of the site. If MySpace.com receives a takedown request from a third party, it determines whether the content in question violates its Terms of Use and takes appropriate action. It also responds to law enforcement requests for data in a manner consistent with U.S. law. Foreign law enforcement requests for data relating to content, as opposed to registration and traffic, continue to be subject to the Mutual Legal Assistance Treaty.

In light of the fact that MySpace.com does not filter or block content based on foreign laws but rather complies with U.S. law we have not joined GNI. However, we are supportive of its work and while we did not participate in the GNI Open House, News Corporation representatives have participated in several GNI related briefings and meetings. Our DC office has a sound working relationship with the Center for Democracy and Technology and engages with it regularly on a variety of issues. We will track the progress of the GNI work stream and provide input as appropriate.

Thank you for your leadership on this important issue and we look forward to working with you to bolster the commitment to the freedom of speech and the privacy of users both in the U.S. and abroad.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Rupert Murdoch", with a stylized flourish at the end.

Rupert Murdoch

NOKIA

OLLI-PEKKA KALLASVUO
President and CEO

February 23, 2010

1 (2)

The Honorable Richard J. Durbin
Chairman, Subcommittee on Human Rights and the Law
United States Senate
Washington, D.C. 20510

DEAR Chairman Durbin,

Thank you for your letter of January 29, 2010 following the allegations of reported Chinese cyber-attacks on Google and other companies. Like many other multinational companies, we are concerned and have been following the situation closely. We appreciate your interest in corporate activities that continue to balance economic and social growth, with the needs to protect human rights and dignities.

Following your August 6, 2009 letter, we did attend the Global Network Initiative (GNI) open house in Washington, D.C. on September 10, 2009. We heard interesting cases and experiences of other companies, and from the GNI about their processes and goals. We continue to monitor the activities of the GNI and are encouraged that they continue to develop their principles based on voluntary action of companies to respect and uphold human rights.

As we described in our August 27, 2009 response to your previous letter, Nokia has for a number of years been engaged in various initiatives by groups focusing on human rights and sustainability efforts. As our participation in those groups has been ongoing, we are comparing and contrasting these initiatives with those of the GNI. Especially in key markets like China, we do proceed with regular business caution and considerable attention to the impact our products have in the market. As previously stated, Nokia believes there is a direct link between mobile technology and economic and social well-being and that by providing people with the means to communicate with one another without regard to where they live or work, we are greatly enhancing the quality of lives of consumers in China and all societies.

Nokia's principal product offering in China is mobile communications devices, which account for more than 99% of our revenues in the market. We have an industry-leading market share in the Chinese mobile device market. Nokia currently operates one manufacturing facility in Beijing, which is geared to high-value, low to medium volume devices; one production facility in Dongguan, which concentrates on the production of high-volume, cost sensitive mobile devices; and a Nokia Research Center (NRC) at Tsinghua University in Beijing. Our manufacturing facilities in China are part of an integrated global production network, giving us flexibility to adjust our production volumes to fluctuations in market demand in different regions.

NOKIA CORPORATION
P.O. Box 226, FI-00045 NOKIA GROUP, Finland
(Street address, Keuholmentie 2-4, 02150 Espoo)

Tel. +359 7180 34474
Fax +359 7180 38683

Business Identity Code 0112038-9
Helsint

NOKIA

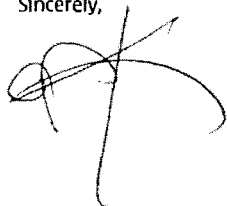
2

The services we currently offer in China are focused on offerings such as Nokia Life Tools (e.g. weather forecasts, agricultural information), mobile education (e.g. English as a second language), "Comes with Music" (music store), and mobile wellness applications (e.g. health information). Generally, these offerings consist of content developed by third-party partners with Nokia acting as an aggregator and distributor. We do not anticipate that the nature of these service offerings will normally implicate human rights issues.

To the extent we face any situations with these or future service offerings that involve any potential human rights issues or government involvement, in China or elsewhere, we will employ the internal processes we described on our response to your earlier letter. We are confident that these procedures will assist us in complying with both our own Nokia values that are embedded on our Code of Conduct as well as well-established international norms for the protection of human rights. We feel that continuing to operate under our internal Code of Conduct, continuing to participate in the Global e-Sustainability Initiative (GeSI), the European Alliance for CSR, and the United Nations Global Compact (UNGC), are the best course of action for Nokia at this time. In addition, we closely follow the work of Professor John Ruggie, the UN Secretary-General's Special Representative on Business and Human Rights, as he is developing a framework for business and human rights. As we described on our previous letter, we will continue to both monitor the development of the GNI and engage in the dialogue with industry and governments about the critically important issue of the protection and promotion of human rights such as freedom of expression and privacy.

I thank you once again for the opportunity to provide Nokia's views on this matter. If you have further questions or need additional information, please contact Leo Fitzsimon, the head of Nokia's Washington, DC office, at leo.fitzsimon@nokia.com, or by phone at (202) 887-0145.

Sincerely,





February 19, 2010

Honorable Richard J. Durbin
Chairman, Subcommittee on Human Rights and the Law
United States Senate
Washington, D.C. 20510

Dear Chairman Durbin:

I am writing in response to your letter of January 29, 2010, which followed closely the revelations regarding alleged cyberattacks on Google and other companies, along with Google's stated intentions to alter the way it does business in China. We appreciate your concern with these developments and applaud your championing of Internet freedoms and human rights.

Your letter requests a description of our business in China. Nokia Siemens Networks ("NSN") has 6,500 employees in China, about 10 percent of our global workforce, working in research and development ("R&D"), and manufacturing, sales, and services of mobile and fixed telecommunications networks. Three thousand of these employees work in our six R&D centers in China. NSN provides mobile networks based on GSM, WCDMA and TD-SCDMA technologies. NSN also is a leading supplier of GSM-R, a radio system for safe and reliable operations of trains, and offers fixed-line infrastructure including equipment for next-generation networks ("NGN"). NSN's customers include China Mobile, China Unicom, China Telecom and China Railway. In 2009, NSN's revenues from China represented approximately 11% of our global business.

NSN believes that the growth and development of communications networks throughout the world plays a significant role in advancing the social, economic and political environment of the relevant communities and countries. Connecting communities and people with each other and the rest of the world leads to many societal benefits.

To that end, NSN is committed to ensuring that all of our employees act, and all corporate decisions are made, in China and in all markets, in a manner consistent with our Code of Conduct. As noted in detail in our letter to you of August 27, 2009, a copy of which is attached, our Code of Conduct includes an absolute commitment to the promotion of fundamental and universal human rights, including freedom of opinion and expression.

Your letter also includes follow up questions regarding the Global Network Initiative ("GNI"). NSN participated in the GNI Open House on September 10, 2009, via teleconference due to the sudden illness of one of the members of our staff. The Open House provided a good opportunity for a range of companies to hear from current participants about their experiences with the GNI. We also heard overviews of the core GNI principles, as well as of the processes involved with the GNI.

NSN has continued and will continue to monitor the progress of the GNI. We believe that the GNI is a laudable effort aimed at addressing concerns regarding privacy and freedom of expression. We share these objectives and take our commitment to them very seriously.

Rajeev Suri
Chief Executive Officer
Nokia Siemens Networks
Email: rajeev.suri@nsn.com

Address: P.O. Box 1
FI-02022 Nokia Siemens Networks
Karaportti 3 FI-02510 Espoo, Finland
Tel +358 718 038 001 Fax +358 718 031 420



In the attached letter, we also highlighted the characteristics of the telecommunications infrastructure industry and explained that NSN is in a vastly different business than the Internet service and application companies comprising the current GNI roster. Unlike those participating in the initiative so far, we do not provide communications services directly to individuals.

We further explained in the attached letter that our industry is global and rapidly evolving. Subsequently, in a clear manifestation of this, at least one industry research firm declared last fall that, at that time, China-based Huawei was the world's second largest supplier of mobile telecommunications infrastructure, behind only market leader Ericsson. NSN, which recently returned to the number two position in the industry, Alcatel Lucent and China-based ZTE round out the global top five. We observed that no telecommunications infrastructure suppliers are members of the GNI. The GNI leadership indicates that the potential exists to adapt the GNI's scope in order to extend it to new market sectors. For such an exercise to succeed, we believe, it will require a full complement of the leading players in each particular sector. In our case, that would include at least all of our major competitors above.

NSN is committed to maintaining a comprehensive approach to human rights issues that best combines effective internal policies, guidelines and procedures with involvement in the most pertinent external programs and organizations. By its nature, this is an ongoing and evolving process, one that we continually evaluate in the context of our unwavering company values. This process includes monitoring and assessing developments with the GNI, as well other relevant initiatives. For example, as we noted in our attached letter, the United Nations Global Compact (UNGC) has a broad and global constituency that includes over 5200 participants from 130 countries representing all industrial sectors committed to following its human rights principles. Both of our corporate parents, Nokia and Siemens, are long-time signatories to the UNGC.

Telecommunications technologies are enabling billions of people around the world to express themselves by communicating with each other, offering their opinions and viewpoints, sharing ideas and organizing around democratic beliefs in new and exciting ways. This global, interconnected nature of communications networks transcends national and regional borders, and is an unstoppable phenomenon. I am extremely proud of the role that NSN plays in helping to make this possible.

Thank you for the inquiry and the opportunity for us to provide information on our business in China and our commitment to supporting human rights globally. If you have any further questions or need additional information, please contact Robert Weisberg, Head of Corporate Affairs for North America, at robert.weisberg@nsn.com, or via phone at (202) 887-0145.

Warmest regards,

Rajeev Suri
Chief Executive Officer
Nokia Siemens Networks

Rajeev Suri
Chief Executive Officer
Nokia Siemens Networks
Email: rajeev.suri@nsn.com

Address: P.O. Box 1
FI-02022 Nokia Siemens Networks
Karaportti 3 FI-02610 Espoo, Finland
Tel: +358 718 038 001 Fax: +358 718 031 420

Page 2 of 2

ORACLE

Oracle Corporation 1015 15th Street NW
 Suite 750
 Washington D.C.
 20005

February 19, 2010

The Honorable Richard J. Durbin, Chairman
 Human Rights and the Laws Subcommittee
 Senate Committee on the Judiciary
 224 Dirksen Senate Office Building
 Washington, D.C. 20510

Dear Chairman Durbin,

On behalf of Oracle Corporation, I'm pleased to respond to your letter in preparation for the Subcommittee's upcoming hearing on Internet freedom in China and around the world. Oracle would like to be as helpful as possible as you undertake your deliberations on this important matter.

As the world's second-largest software company, Oracle does business throughout the world -- including China -- and we provide mission critical software and hardware components for governments and medium-sized to large businesses. Our business consists largely of "infrastructure" software, such as operating systems, database and middleware; applications software, such as supply chain and accounting; and high-end servers. Oracle has never been in the consumer business and as such has very little involvement with consumer information, personally identifiable or otherwise.

While Oracle customers utilize our technology and applications to access, manipulate and store large amounts of business, sales, employee, customer, and consumer data, Oracle itself typically has no control over this information. In fact, when we license our infrastructure technology to a customer, we have little means to know what processes they may be running, what types of information they may be storing and how they are using that information. In some limited circumstances, customers may choose to have Oracle host and maintain their applications, but in those cases all of that data is stored at our secure server farms at our facilities in the US. Moreover, this data would be structured information (customer #'s, contact information), and not the type of personal communications we assume the Committee is primarily concerned with. Thus, even in our hosted solution the type and location of the information make it highly unlikely that unauthorized parties could access information for the purposes under consideration by the committee.

Our technology plays an extremely limited role in interfacing directly with consumers and Internet users and, as such, Oracle has not developed specific measures to ensure that our products and services do not facilitate human rights abuses by the Chinese government. In our ordinary business dealings in China and elsewhere, it would be extremely unlikely that the type of information we may have access to could form the basis of human rights abuses, and even less likely that we would be able to exert control over any enterprises that conducted such activities. Moreover, as an enterprise software company with a specific contractual relationship with each one of our customers, Oracle has developed a Code of Ethics and Business Conduct, to ensure

February 19, 2010

Page 2

that Oracle employees operate within the bounds of all laws, regulations, and internal policies applicable to Oracle's business, wherever we conduct it, including in China.¹

Regarding the Global Network Initiative (GNI), as you correctly point out, this initiative regards "Internet and communications firms," not enterprise infrastructure vendors such as Oracle. Oracle was not invited nor did it play any role in formulating these principles as these were appropriately developed by companies who retain personal information and organizations established to protect consumer privacy and international human rights. As a result, while we certainly support the goals of the GNI, the specifics really do not reflect the manner in which we do business or the way our technology is practically deployed.

Thank you for the opportunity to respond to this inquiry. Please let me know if we can be of further assistance.

Sincerely,



Jason M. Mahler

Vice President, Government Affairs

¹ The Committee is aware that software piracy continues to be a major problem in China and as such we cannot guarantee that we know precisely who is using which Oracle products.

ORACLE®

DICKSTEINSHAPIRO LLP

1825 Eye Street NW | Washington, DC 20006-5403
 TEL (202) 420-2200 | FAX (202) 420-2201 | dicksteinshapiro.com

February 19, 2010

Via Electronic and U.S. First-Class Mail

The Honorable Richard J. Durbin
 Chairman, Subcommittee on Human Rights
 and the Law
 Senate Committee on the Judiciary
 United States Senate
 224 Dirksen Senate Office Building
 Washington, DC 20510

Dear Chairman Durbin:

I am writing on behalf of my client, McAfee, Inc. ("McAfee"), in response to your letter dated January 29, 2010. Below please find McAfee's responses to the questions posed in your letter concerning its business in China, future plans for protecting human rights in China, and the Global Network Initiative ("GNI"). As demonstrated below, McAfee is strongly committed to human rights, including privacy and freedom of expression, and appreciates your interest in these issues.

1. Please provide a detailed description of your company's business in China.

McAfee's business in China is fundamentally in the nature of a start-up enterprise. Sales to consumers constitute a major percentage of McAfee's revenue in China. Indeed, 40 percent of McAfee's business in China derives from selling to consumers a basic anti-virus product to protect personal PC's; the company also sells this product to foreign multi-nationals, as well as small and medium-size businesses. Additionally, McAfee markets its standard, commercial-grade filtering technology to private-sector customers in China. This filtering technology enables customers to screen the web for material that they might find inappropriate for their homes or businesses, such as pornography or gambling websites. This is the same technology McAfee sells to consumers around the world, although it accounts for a very small percentage of McAfee's total revenues. Collectively, these technologies enable millions of Chinese consumers and companies to obtain information and conduct business safely and productively.

According to such industry analysts as Gartner, the Chinese IT market will soon become the largest in the world. American IT companies must have a presence in this market to remain competitive in a global market that rewards companies that achieve economies of size and scope, and punishes companies that fail to achieve these bench marks. McAfee is focused on building a competitive business in China, in large part to keep pace with many of its larger competitors, including Symantec and Cisco, that have already achieved business presence and success in China. To that end, McAfee is in the process of setting up a joint venture which will enable it to manufacture products in China.

Washington, DC | New York, NY | Los Angeles, CA

DICKSTEIN SHAPIRO LLP

The Honorable Richard J. Durbin
 February 19, 2010
 Page 2

McAfee currently does very little business with the Chinese government. While McAfee does limited work for several state-owned entities, including a Hong Kong-based subsidiary of Bank of China, as well as partnerships with China Unicom and China Telecom, McAfee has not obtained the certifications required to secure the licenses needed to do business with government agencies. Moreover, it is unlikely that McAfee will be willing or able to obtain such certifications, since that would require McAfee to, among other things, reveal all source codes. It is worth noting that few U.S. security companies are able to win government business in China due to the preference officials have given to Chinese security companies. Consequently, the Chinese government market is not a particularly attractive opportunity for many American security companies.

2. What are your company's future plans for protecting human rights, including freedom of expression and privacy, in China? Please describe any specific measures you will take to ensure that your products and/or services do not facilitate human rights abuses by the Chinese government, including censoring the internet and monitoring political and religious dissidents.

McAfee is committed, at all levels of the company, to protecting freedom of expression and privacy as we attempt to expand our businesses in China. In no event will McAfee knowingly assist the Chinese government in blocking any specific content or any specific web sites.

McAfee's commitment to human rights and freedom of expression in China is perhaps best evidenced by its recent efforts to assist Google and approximately 20 other companies, as well as the United States government, through a forensic investigation into the "Operation Aurora" cyber attack, which Google has said publicly was aimed at hacking the Gmail accounts of Chinese human rights activists. As part of its investigation, McAfee analyzed several pieces of malicious code and confirmed that they were used in attempts to penetrate several of the targeted organizations. McAfee's briefings proved to be invaluable to the United States government, and McAfee's Global Threat Intelligence service — a unique offering that allows the company to constantly monitor and plot solutions to cyber threats, regardless of where they might originate — enabled it to share important new information with key government agencies. McAfee is continuing to work with multiple organizations that were impacted by this attack, as well as government and law enforcement agencies, to address this major attack.

McAfee also has specific policies and procedures in place to protect human rights and freedom of expression. McAfee's most significant relevant product is its SmartFilter® web filtering software, which consists of the actual off-the-shelf software, as well as regular access to the SmartFilter® database. SmartFilter® classifies Internet content into nearly 100 different categories so that customers can choose, by category, what types of web content they want made available to their organization. For example, SmartFilter® is widely used by schools to ensure pornographic websites are not being viewed by children. Corporations use SmartFilter® as a productivity tool, blocking content such as celebrity gossip websites. McAfee deliberately does not provide any categories that are intended to assist a user in discriminating on the basis of race, religion, political persuasion, gender, sexual orientation, or any other personal characteristics.

DICKSTEIN SHAPIRO LLP

The Honorable Richard J. Durbin
 February 19, 2010
 Page 3

McAfee is in the process of developing a comprehensive set of human rights impact assessment guidelines to inform its strategic business decision-making process, and intends to begin implementing these guidelines later this year. The impact assessment focuses on privacy and freedom of expression issues, and includes in-depth analysis of high risk areas, potential risk mitigation strategies, and ongoing monitoring.

In response to the Committee's initial letter, McAfee recently added a specific provision concerning privacy and freedom of expression in its Code of Business Conduct: "McAfee and its employees are deeply committed to the principles of privacy and freedom of expression. We will strive to advance these principles as we develop and market new and existing products and services in diverse business environments around the world."

Furthermore, McAfee's Employee Handbook and Code of Business Conduct emphasize the importance of privacy and confidentiality. The relevant portion of the Employee Handbook, for example, states in part: "Use of personal information may be subject to legal restrictions, and also may be subject to specific preferences and/or requirements requested by the customer, partner, and/or supplier. Respecting expressed privacy preferences and requirements is important to our competitive position in the industry, and in certain geographies it is required by law." The Code of Business Conduct provides: "Directors, officers and employees must maintain the confidentiality of confidential information entrusted to them by the Company, its customers, partners, distributors and suppliers, except when disclosures are specifically authorized by the Legal Department or required by law."

3. Did representatives of your company attend the GNI open house? If no, why not?

McAfee representatives attended the GNI open house on September 10, 2009, and were active participants in the discussion. Additionally, to the best of our knowledge, McAfee has participated in every conference call that GNI has organized since that time — November 18, 2009, and December 16, 2009.

McAfee has been actively engaged with the GNI because GNI has been instrumental in raising awareness of, and expanding the dialogue on, the impact of technology on human rights issues. McAfee supports GNI's stated purpose of encouraging companies to examine, as part of the regular strategic decision-making process, whether and to what extent their products and services may be used to limit freedom of expression and access to information.

DICKSTEINSHAPIROLLP

The Honorable Richard J. Durbin
February 19, 2010
Page 4

4. Does your company plan to participate in the GNI work stream? If no, why not?

McAfee has been actively participating in the GNI work stream, and will continue to do so. To that end, McAfee held its first one-on-one discussion with a GNI representative on January 27, 2010. This conversation was a constructive opportunity for McAfee to ask questions regarding GNI's policies and procedures, to describe the functionality of McAfee's products, and to address basic concerns. McAfee looks forward to participating in the GNI Implementation Dialogue to be held in March 2010.

Please do not hesitate to contact me at (202) 420-3447 if you have any questions.

Sincerely,



Mark R. Paoletta
Partner
Dickstein Shapiro LLP
1825 Eye Street N.W.
Washington, DC 20006
Tel: (202) 420-3447| Fax: (202) 420-2201
paolettam@dicksteinshapiro.com



February 19, 2010

Senator Richard Durbin
309 Hart Senate Building
Washington DC, 20510

Dear Senator Durbin,

I am writing in response to your letter of January 29, 2010 to Research In Motion Limited. Co-CEO, Mike Lazaridis. Thank you for the opportunity to provide information about our company and our business in China.

As you know, RIM is the designer and manufacturer of the BlackBerry mobile communications platform. The BlackBerry solution incorporates smartphones, software and wireless services and is available from more than 500 wireless operators and other distribution partners in more than 175 countries.

BlackBerry provides mobile professionals and consumers with convenient and robust access to email, messaging, and voice services as well as a wide range of mobile applications. RIM's BlackBerry Enterprise Service (BES), widely deployed by corporations and government organizations, was specifically designed to protect sensitive information in its most vulnerable state: while moving over the public airways between a corporate or government data center and a smartphone. The BlackBerry Internet Service provides consumers with a level of assurance commensurate with their requirements as citizens in an electronic world.

The security model of the BES solution has been certified by major government and private organizations including the United States National Institute of Standards and Technology, the Fraunhofer Institute for Secure Information Technology in Germany, and the Communications Electronic Security Group in the United Kingdom. BES is certified to the U.S. Federal Information Processing Standard 140-2 (FIPS 140-2) and it has also achieved Common Criteria EAL Level 4+ certification. Additional details may be found at: www.blackberry.com/security.

Since 2006, RIM has provided the BlackBerry Enterprise Solution to business customers in China with operator wireless service provided by China Mobile. The solution marketed in China is identical to that available in every country we serve.

In addition, the BlackBerry solution for business will be available soon through China's second-largest wireless operator in terms of revenue, China Telecom. Later this year, RIM plans to launch the consumer-oriented BlackBerry Internet Service with our China operators.

Research In Motion Corp. 1300 Eye Street, NW, Suite 1000 West Tower, Washington, DC 20005 tel. (1) 202-204-4659 web: www.rim.com

02/21/2010 6:21PM

2010-02-21 07:33

12025182518 >> US SENATE

P.3/3

To Senator Richard Durbin

February 19, 2010

Page 2

RIM's engagement in China also includes sponsorship of graduate research at five universities and work with the local developer community to bring more localized content and applications to the BlackBerry platform for Chinese customers. In 2007, RIM received the "Contributor of Chinese Enterprises' Information Award" in recognition of efforts in developing enhanced communication and information technology in China.

RIM has built a global business by remaining steadfast to the principle that sensitive information sent over public airways must be free from unlawful hacking, interception and other malfeasance. We also believe that the systems that deliver such information must be free from viruses and other malware.

Thank you again for the opportunity to comment. I would also welcome the opportunity to meet with you or your staff to provide further information about security on the BlackBerry platform. Please feel free to contact me if I can be of further assistance.

Sincerely,



Robert E. Crow, Vice President
Industry, Government & University Relations
Research In Motion Limited

Research In Motion Corp. 1300 13th Street, NW, Suite 1000 West Tower, Washington, DC 20005 tel: +1 202-204-4659 web: www.rim.com

02/21/2010 6:21PM



February 19, 2010

The Honorable Richard J. Durbin
Room 309 Hart Senate Building
United States Senate
Washington, DC 20510

Dear Chairman Durbin:

Thank you for your letter regarding Internet freedom in China and around the world.

At SAP, we are deeply committed to running our business in a responsible manner consistent with the principles of ethics and sustainability, including a commitment to human rights. Responsible values and the highest standards are at the heart of our products and services, which enables our customers to greatly improve the transparency, accountability, and sustainability of their operations.

Over the years, SAP has collaborated in several initiatives that have dealt with human rights. For example, since 2003 SAP has been an active member of the UN Global Compact, which brings together businesses that are committed to aligning their operations and strategies with universally accepted principles in the areas of human rights, labor, environment and anti-corruption. SAP has also been active in the Global Reporting Initiative in its development of standards that organizations can use to publicly report their social and environmental performance.

Internally, SAP has a global team sponsored by senior management with a mandate to oversee all aspects of sustainability across our business, including solutions development, environmental performance (both in our software and SAP's internal operations), economic impact, and social performance including human rights, labor practices, and SAP's relationship with society. Further information about our governance, sustainability, and corporate social responsibilities efforts can be found online at <http://www.sap.com/about/csr/index.epx> and <http://www.sap.com/about/SAP-sustainability/index.epx>.

With regard to the specific issues you raise, it is important to understand the nature of our business. SAP is the world's leading provider of business software solutions, helping public and private sector organizations manage functions such as financial accounting, enterprise resource planning, human resources, supply-chain coordination, and legal compliance. SAP does not provide Internet services, networking equipment or services, or telecommunications equipment or services; and thus SAP is not directly involved in matters of Internet freedom.

SAP has had operations in China since 1995, and today serves hundreds of public and private sector customers with a wide array of SAP products and services. SAP China employs approximately 2,500 people, most of whom are local hires. SAP Labs China, located in Shanghai, employs 1,200 people who develop functionality and modifications to SAP software for the Chinese business market, just as other SAP regional labs localize our products for their regions' needs.

Regarding the Global Network Initiative (GNI), SAP has not been actively involved in this effort because we are not an Internet services or network services provider. However, the GNI's principles are consistent with SAP's own principles and values, and we will continue to follow the progress of GNI's implementation dialogue.

Senator, before closing, I would like to mention that SAP America has more than 9,400 employees in the United States, including nearly 800 in Illinois, and we pay an average salary that is well above the national average. At a time when the entire country is concerned about jobs and solid careers, we are proud of our jobs growth in the United States in recent years. In addition, SAP's University Alliance annually gives more than \$100 million in in-kind donations and grants to US schools and universities, including Southern Illinois University in Edwardsville, to develop the next generation of business and technology leaders.

Thus, we are proud to say that SAP is a global company with a strong commitment to helping people in every market we serve -- including the United States and China -- and to upholding human rights, sustainability, and the highest ethical standards in all that we do.

Thank you again for the opportunity to share our views on issues of mutual concern.

Sincerely,



WRM/br

SIEMENS

The Honorable Dick Durbin
Chairman
Subcommittee on Human Rights and the Law
Committee on the Judiciary
U.S. Senate
Washington, D.C. 20510

Dear Chairman Durbin:

This is to respond to your letter of January 29, 2010 concerning your upcoming hearing "Global Internet Freedom: Corporate Responsibility and the Rule of Law," requesting a description of our business in China, and information relating to Siemens principles and business conduct guidelines.

I have enclosed a presentation that we use to describe our business in China. In summary, our business includes businesses in three sectors: Industry, Energy, Healthcare. Industry includes: industry automation; drive technologies; building technologies; lighting; rail. Energy includes: fossil power generation; renewable energy; oil, gas and energy services; power transmission; power distribution. Healthcare includes: imaging and IT for hospitals; workflow and solutions; diagnostics. In addition, we provide some financial services and networking (intra-company) solutions and services.

Siemens workforce in China is approximately 43,000, with business totaling approximately 57 Billion RMB yearly.

As we mentioned in our September letter, Siemens no longer has operational or managerial control of any information and communications technology company (ICT), and therefore our view is that the Global Network Initiative is not directly applicable to our business. Siemens, as a global company, is dedicated to strong corporate responsibility initiatives and business conduct principles. I have enclosed a copy of our letters dated September 2nd, 2009 outlining our business practices that align with and extend beyond the human rights principles included in the Global Network Initiative.

Thank you for the opportunity to explain our business in China and Siemens' dedication to responsible business conduct. I hope that this responds to your request for information. Please do not hesitate to contact me at any time via email, kathleen.ambrose@siemens.com, or via phone at (202) 434-4835.

Sincerely,



Kathleen Ambrose
Senior Vice President, Government Affairs
Siemens Corporation

Siemens Corporation

601 Pennsylvania Avenue, N.W.
North Building, Suite 1100
Washington, DC 20004-2601

Tel: (202) 434-4800
Fax: (202) 347-4015



February 18, 2010

Senator Richard J. Durbin, Chairman
U.S. Senate Committee on the Judiciary
Subcommittee on Human Rights and the Law
224 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Durbin:

Thank you for your letter of January 29th regarding the recent 'Chinese cyber-attack' on Google and other companies and on-going efforts to safeguard freedom of expression and privacy across the globe. Over 560 million people around the world utilize Skype's software for their conversations. We strive to ensure that consumers can use Skype to reach friends and loved ones, particularly where no other communications options are available. More and more people around the globe, from the US to Europe to Haiti to Iran, are turning to technologies like Skype to freely connect with one another across borders and to increasingly facilitate interaction and understanding.

As I expressed in my letter to you this past summer, I am deeply committed to Skype's mission to enable the world's conversations and I continue to share your concerns about the efforts of governments to arbitrarily violate core privacy rights. We appreciate the opportunity to discuss these important issues with you. Skype's answers to the specific questions you pose in your letter are set forth below.

Allowing the world to communicate for free empowers and links people and communities everywhere. We believe that our software empowers citizens globally by providing greater freedom of expression and access to information, and is central to the Freedom to Connect, as articulated by Secretary of State Hillary Clinton in a recent address regarding human rights and Internet freedom. Our challenge is to provide our software to people all over the globe, including in Internet restricting countries, while being transparent to our users and staying within the boundaries of applicable local laws. Nearly 1 in 6 people in the world live in China and a great many of them rely on Skype to connect with families and friends, run businesses, and call people around the world. By and large, people in China are able to do this for free. We believe that to deny users in China access to Skype would be to deny their Freedom to Connect.

As a Luxembourg-based company, our primary efforts to protect free speech and privacy rights for the Skype user community have been based, in the first instance, on Luxembourg law. However, where we have a local presence, we need to take account of applicable local laws and regulations. Further, mindful of the need to avoid multiple, overlapping jurisdictional mandates, we are focused primarily on European initiatives that seek to enshrine the same or similar principles as the

Skype Communications S.à r.l.
6ème étage, 22-24 Boulevard Royal, L-2449 Luxembourg, Grand-Duché de Luxembourg +352 2663 9130 +352 2553 9150
Registered in the RC Luxembourg B103.499





Global Network Initiative (GNI). Specifically, Skype has focused primarily on the activities of the Council of Europe (CoE). The CoE is currently working to address practical ways for European companies to comply with human rights obligations and establish relevant best practices for European Internet Service Providers and other Information Society companies. The CoE efforts are based on a collaborative process with the European Internet Services Providers Association (EuroISPA), the world's largest ISP organization, including Internet service providers (ISPs) who provide access services and other information society providers including web hosting, application, and content providers. Together, the CoE and EuroISPA issued guidelines based on the high standards of the European Convention on Human Rights to provide human rights benchmarks for ISPs and other providers in the Internet ecosystem. In fact, Skype has worked to arrange meetings between the current company members of the GNI and the CoE in an attempt to facilitate a deeper understanding and cooperation between the two organizations regarding their overlapping missions. We will continue to act as a facilitator for such cooperation in future.

To address your specific questions about Internet freedom and human rights in China:

1. First, in your letter you ask us to provide a "detailed description of your company's business in China."

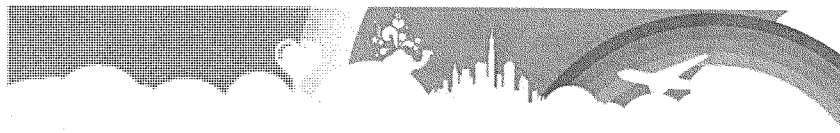
Skype is a Luxembourg-based company doing business via the global public Internet. As such, Skype does not have any direct operations in China. Skype is a minority partner in a joint venture in China. Skype is represented in China through the majority joint venture partner, TOM Online – a Hong Kong based company with substantial local operations and assets and part of the Hutchison Whampoa Group. The joint venture was formed in 2005. As the local and majority partner, TOM has undertaken responsibility for all government relationships with the Chinese authorities. Skype has not had any interaction with the Chinese government. Skype does not have an office nor employ any staff in China. Our relationship with TOM, including oversight of the joint venture, is managed from our Luxembourg headquarters and regional support offices.

TOM distributes a localized version of the Skype software that brings the Skype experience to Chinese residents and provides greater relevance to the local market. Like any other communications company in China, TOM has established procedures to meet local laws and regulations, including the obligation to cooperate with lawful criminal investigations and to protect public safety, which in the case of the TOM-Skype software includes a requirement to perform text filtering on instant messaging. Separately, Skype makes available a Mandarin version of the global Skype software, which is different from the localized TOM version. Unlike the localized version, the Skype Mandarin version does not include text filters such as those applied to the TOM-Skype client. It is available for download worldwide.

- 2 -

Skype Communications S.à r.l.
6ème étage, 22-24 Boulevard Royal, L-2449 Luxembourg, Grand-Duché de Luxembourg T +352 2803 9130 F +352 2803 9850
Registration no. 82 Luxembourg 850-498





2. Second, you ask "what are your company's future plans for protecting human rights, including freedom of expression and privacy, in China? Please describe any specific measures you will take to ensure that your products and/or services do not facilitate human rights abuses by the Chinese government, including censoring the Internet and monitoring political and religious dissidents."

I am proud of Skype's efforts to enable our users to have safe and secure voice conversations via Skype. Skype undertakes responsible company decision-making and incorporates, as far as is practical and with due respect to applicable local laws, the fundamental tenets of free expression and the right to privacy in our business practices. First and foremost, as stated above, Skype continues to make available a Mandarin-version of our software that is not subject to the text filtering. In other words, the issues of Chinese authorities requiring local providers in China to filter text messages do not affect communications where all parties are using standard Skype software. Filtering occurs only in the context of instant messaging communication in which one or more parties are using the co-branded TOM-Skype client software. We are able to uphold freedom of expression and the right to privacy of Skype users by simultaneously offering the Mandarin version of our software. We also believe that the content of Skype-to-Skype voice or video conversations in China remain secure and private.

As stated previously, in addition to making the Mandarin version of Skype available, we are continually improving Skype's business operations to protect and safeguard freedom of expression and privacy while ensuring that our users can continue to access the Skype software and communicate across the globe. Specifically, Skype, in our constant attempt to be open and transparent with our users as to how their personal information is processed:

- has modified our security and privacy web pages, which can be found at <http://www.skype.com/security/detailed-security/faq/>, to provide clear and transparent guidance to our users about possible compromises in the security integrity of communications when the software is a version provided by a third party or the communications traverse third party networks;
- is working with TOM to link to a Mandarin version of the Skype security and privacy pages from the TOM web pages to increase local transparency;
- gathers and retains only minimal personal information about our users thereby minimizing risk should a security breach occur;
- has established clear procedures for engaging with law enforcement authorities across the globe in accordance with Luxembourg law; and
- is in conversations with TOM to delineate more clearly their procedures for engaging with Chinese authorities.

- 3 -

Skype Communications S.à r.l.
8ème étage, 22-24 Boulevard Royal, L-2449 Luxembourg, Grand Duché de Luxembourg T +352 2663 9130 F +352 2663 9550
Registration no. RC Luxembourg 010/498





In addition to these precautions, as stated previously, we believe that all Skype-to-Skype conversations utilizing the standard Skype software are fully encrypted, and thus secure and private during transmission. Skype is acutely conscious of the need for transparency, consistency, and honesty in how we address the issue of the right to freedom of expression and privacy while maintaining the delicate balance with delivering upon law enforcement and security agencies' legal mandate to pursue criminal and terrorist investigations. We currently achieve this through the encryption and privacy protections that are built into the Skype software, and note that these protections are superior to those offered by traditional telecommunications firm operating in China or across the globe.

In addition to the questions above about China, you go on to ask questions about Skype's involvement with GNI. I am pleased to report that since our response to your August 2009 letter, we have continued a productive and informative dialogue with the members of GNI. Specifically,

1. You ask whether "representatives of your company attended the GNI open house on September 10, 2009."

Skype participated in the GNI open house on September 10, 2009 as well as several additional follow up meetings and conference calls, including: calls to organize meetings in Europe with similarly situated European companies, followed by a meeting in Paris between GNI and Skype's Directors of Government and Regulatory Affairs for North America and Europe and the Middle East; a November 5, 2009 GNI open house in Singapore with Skype's Director of Government and Regulatory Affairs for Asia; and a GNI Implementation Dialogue in December 2009.

While these meetings have been helpful in highlighting those areas of the GNI governing documents that require clarification for Skype, there are a number of factors that we continue to work on with GNI to ensure that we have sufficient information to make a reasoned and informed decision regarding the merits of memberships. These include, as discussed above, our current efforts to balance competing or overlapping requirements in multiple jurisdictions across the globe, as well as our desire to understand thoroughly the impact on our business operations associated with GNI membership. We do not take the responsibilities associated with membership in GNI lightly and will only join after appropriate due diligence, which can be time consuming. As the current members of GNI have recognized during the course of the meetings last year, it is critical that the governing documents are sufficiently flexible to enable compliance by a range of companies regardless of their geographical location, corporate structure or business mission. Through this engagement, Skype has gained a more precise understanding of the various stakeholder positions in GNI and the impact of the governing documents on member companies.

2. Second, you ask whether Skype "plan[s] to participate in the GNI workstream."

- 4 -

Skype Communications S.à r.l.
Bâle étage, 22-24 Boulevard Royal, L-2449 Luxembourg, Grand-Duché de Luxembourg
T +352 2663 9150 F +352 2663 9550
Registration no. RC Luxembourg 0900468





As stated above, Skype's dialogue with GNI has been on-going and informative. We have participated in multiple meetings, including the initial workstream meeting highlighted in your letter, and plan to participate in the upcoming GNI Implementation Dialogue scheduled for March 9, 2010. Cooperative efforts such as the workstream are the primary tools necessary to ensure a full understanding of the obligations of GNI membership and the potential modifications or clarifications that might be entertained by the current membership. It is important to continue this dialogue and to include other non-US based as well as smaller/early stage companies that are similarly situated to Skype. It is our hope that these meetings will result in concrete proposals for clarifications and modifications to the GNI guidelines to make them appropriate for non-US and smaller/early stage businesses.

Thank you again for your thoughtful letter. Skype is committed to ensuring that users of communications and information technology tools across the globe are not stymied by arbitrary threats to privacy and freedom of expression. We must all work together, governments and industry alike, to ensure that the Internet continues to be a tool for free expression and innovation everywhere in the world. We look forward to continuing this productive dialogue with your office, GNI members and the CoE.

Respectfully,

Josh Silverman
CEO

SKYPE COMMUNICATIONS S.A.R.L.
6e etage, 22/24 boulevard Royal,
Luxembourg, L-2449 LUXEMBOURG

- 5 -

Skype Communications S.à r.l.
6ème étage, 22-24 Boulevard Royal, L-2449 Luxembourg, Grand-Duché de Luxembourg
T +352 2663 9130 F +352 2663 9550
Registration no. RC Luxembourg 8109 408





Vonya B. McCann
Senior Vice President
Government Affairs

Sprint Nextel
Suite 700
900 7th Street, NW
Washington, DC 20001

February 19, 2010

CONFIDENTIAL

The Honorable Richard J. Durbin, Chairman
Subcommittee on Human Rights and the Law
Senate Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Durbin:

Thank you for your letter of January 29, 2010 inquiring about Sprint Nextel Corporation's ("Sprint") business in China and possible participation in the Global Network Initiative ("GNI").

Sprint does not typically confront the human rights issues that the GNI seeks to address, given the nature and scope of its network operations overseas. Outside of the United States, Sprint has deployed an Internet Protocol ("IP") wireline network in countries where the type of freedom of expression and privacy issues over which the GNI is concerned do not normally arise. Moreover, within such countries, Sprint's business is generally limited to providing private IP communications network services to U.S.-based multinational companies, which use our services to link their U.S. and foreign offices together. Sprint does not offer Internet access service to individual foreign end users located within those countries. Against that backdrop, below please find responses to your specific questions.

(1) Please provide a detailed description of your company's business in China.

Sprint neither provides communications service nor operates a communications network within mainland China. Consequently, Sprint business enterprise customers requiring service to sites in mainland China receive such service from licensed Chinese communications carriers.

(2) What are your company's future plans for protecting human rights, including freedom of expression and privacy, in China? Please describe any specific measures you will take to ensure that your products and/or services do not facilitate human rights abuses

Office: (202) 585-1902 Fax: (202) 585-1940 vonya.b.mccann@sprint.com

The Honorable Richard J. Durbin, Chairman
February 19, 2010
Page 2

by the Chinese government, including censoring the Internet and monitoring political and religious dissidents.

Since Sprint neither provides communications service nor operates a communications network within mainland China, Sprint has no such plans specific to China. As a general matter, however, Sprint respects the fundamental principles of freedom of expression and privacy in conducting its overall operations. Sprint seeks to ensure that its users' freedom of expression is not restricted improperly. Furthermore, Sprint is committed to protecting the privacy of the personal information it collects and taking steps to protect it against unauthorized access or disclosure.

(3) Did representatives of your company attend the GNI open house? If no, why not?

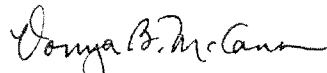
Yes, two Sprint representatives attended the GNI Open House held in Washington, D.C. on September 10, 2009.

(4) Does your company plan to participate in the GNI workstream? If no, why not?

Sprint supports fully the laudable goals and objectives of the GNI. Since Sprint does not normally encounter human rights-related issues, however, it does not plan to participate in the GNI workstream at this time. Subject to further evaluation, Sprint may consider participating if it begins to confront these issues in the normal course of its international business operations. In the meantime, Sprint looks forward to closely monitoring the GNI's continued progress and engaging with the GNI as a key resource for information.

Thank you again for your inquiry.

Sincerely,



Vonya B. McCann
Senior Vice President, Government Affairs



February 19, 2010

Senator Richard Durbin
United States Senate
309 Hart Senate Building
Washington, DC 20510

Senator Durbin,

Thank you for your letter. We share your interest in the important issue of internet freedom and are eager to express our opinion in this response. Indeed, our company was founded on the belief that the open exchange of information has a positive effect on the world. Our product and business decisions in Twitter's short existence have been inspired by that belief.

This begins with the simplicity and openness of Twitter. We've limited our messaging system of "Tweets" to 140 characters of text, with no images, video or other files. That means that people with the most rudimentary mobile phones around the world can tap into Twitter's functionality via SMS.

We also decided from the start to make Twitter open to improvements and innovations from both users and third party developers. It's for that reason that Twitter, the company, seems much bigger than it actually is. We have greatly benefited from the energy and momentum of thousands of developers who have freely tapped into our system and have created more than 50,000 applications that allow our users to send and receive Tweets on a vast array of devices, web services and software programs.

The innovation and rapid growth of Twitter's developer community has had a dramatic impact on global communication but we are constantly reminded that Twitter is a triumph of humanity -- not technology. Credit goes to the brave and dedicated individuals who tapped the power of Twitter during the aftermath of last years Iran election; the steadfast human rights activists in China working around blocks of the service; and the opposition efforts currently underway in Venezuela who dare use what President Hugo Chavez calls a "terrorist" tool. While the potential of Twitter has not yet been realized, these early examples show how important information can find its way from one restless area of the world to engage a much bigger audience.

For Twitter to reach its potential as a democratizing service we need to keep a steadfast focus on building a scalable service and a sustainable business. When the Iran election happened last summer, Twitter only had about 30 employees and struggled to keep the site up during the protests (which caused the State Department to request the postponement of a critical fix to the service). We're growing, but on relative terms to other big internet

players, we are still tiny, with less than 150 employees (as compared to the tens of thousands of employees at companies such as Google, Yahoo! or Cisco). At our size, nearly everyone in our company is working long hours to ensure that Twitter keeps up with user demand to increase the chances that information can be shared in current global hot spots and ones not yet considered.

We also need help through the leadership and action of Congress and the Obama administration. We greatly applaud your efforts to that end and also hope that Secretary Clinton's recent speech on internet freedom is followed by continued administration action.

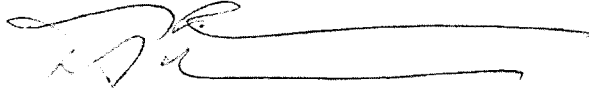
Specifically, we believe that the free and open exchange of information would benefit enormously from limits on the abilities of governments and private parties to require service providers to remove information or to respond to requests to reveal user information. Even though we only operate in the United States, we face significant challenges in these areas both domestically and internationally. We have been sued for not removing information both in the United States and Brazil and we expect more litigation. In other countries, such as China, even though we have neither received nor responded to any removal or information requests, we believe that we have been technically blocked. We appreciate the United States government's willingness to engage with those countries in order to end such speech suppressive blocking.

Though we have spoken with a number of advocacy groups with respect to internet freedom issues, we have not had the luxury of time to be able to fully evaluate GNI. It is our initial sense that GNI's draft policies, processes and fees are better suited to bigger companies who have actual operations in sensitive regions. Nevertheless, we will continue to evaluate GNI along with other organizations, such as the Chilling Effects Clearinghouse (<http://www.chillingeffects.org/>), as we maintain our focus on helping our users freely express themselves.

Finally, Twitter greatly appreciates your invitation to speak at the March 2 hearing. It would be an excellent opportunity for Twitter to tell our story to a supportive audience given our shared beliefs regarding internet freedom. However, as I discussed with your staff, we are simply still too small a company to be able to deal with the increase in Washington exposure that participating in such a hearing would cause. We hope that you understand that we are focused on making our service better and more reliable rather than speaking about our record promoting freedom of speech. For that reason, we have declined all such appearances and ask that you accept our sincere apology in declining yours as well.

I appreciate the opportunity correspond with you about Twitter. Also, please accept my apologies that we did not receive your previous letter.

Sincerely,

A handwritten signature in black ink, appearing to read 'A. Macgillivray', with a long horizontal flourish extending to the right.

Alexander Macgillivray
General Counsel
Twitter, Inc.

Kathryn C. Brown
Senior Vice President
Public Policy Development &
Corporate Responsibility

February 19, 2010

The Honorable Richard J. Durbin
Chairman
U.S. Senate Committee on the Judiciary
Subcommittee on Human Rights and the Law
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Durbin:

Thank you for your January 29, 2010 letter to Mr. Seidenberg regarding your plan to convene a hearing of the Human Rights and the Law Subcommittee to focus on Internet freedom around the world, particularly in light of Google's recent announcement that it will no longer censor its China search engine. Mr. Seidenberg has asked me to respond on behalf of Verizon. Your letter asks for information on our business in China, and what measures we will take to ensure that our products and services offered there do not facilitate human rights abuses by the Chinese government. Your letter also asks about our participation in the September 10, 2009, Open House on the Global Network Initiative (GNI) and a subsequent workstream.

At the outset, we once again commend your leadership in advancing human rights internationally and addressing the challenges to Internet communications in China and around the world. As a participant in the global Internet ecosystem, Verizon shares your belief that preserving the ability to communicate over the global Internet is an important issue for human rights, the global economy, and democracy everywhere. Secretary Clinton's recent remarks on Internet freedom rightly recognized that government-to-government actions are critical to averting and addressing abusive foreign government policies relating to freedom of expression and privacy. It is our hope that her leadership on behalf of the U.S. government will lead to more discussions and development of shared norms among nations in multilateral venues.

We also recognize that businesses have an important role to play, and we at Verizon are committed to supporting human rights values and to being a positive force in society wherever we do business. Our commitment to protect human rights is expressed in our corporate policies and practices, which include support for freedom of expression and privacy. Specifically, we have issued a Human Rights Statement (<http://responsibility.verizon.com/home/approach/human-rights>) which acknowledges the importance of the broad principles expressed in the United Nations Universal Declaration of Human Rights. Verizon's support for the important principles of freedom of expression and protection of privacy are encapsulated in our Guiding Principles for Content on Verizon Networks (www.verizon.com/contentpolicy) and Privacy Policy (<http://www.verizon.com/privacy/>), respectively, both of which are publicly available. These statements embody Verizon's commitment to furthering human rights and to our customers' rights and privacy, consistent with our legal obligations as a provider of communications



1300 I Street, N.W., Suite 400 West
Washington, DC 20005

Phone 202 515-2407
Fax 202 336-7914
kathryn.c.brown@verizon.com

The Honorable Richard J. Durbin
February 19, 2010

Page Two

services in jurisdictions around the world. Verizon is also committed to engaging constructively with policymakers, members of the Internet community, and other stakeholders to further these goals. We look forward to participating in the upcoming work of the Global Internet Freedom Task Force convened by the Department of State.

Your letter asks specific questions about Verizon's business in China and the Global Network Initiative (GNI). Our responses to each question follow.

- Verizon's Business Operations in China. You have asked that we describe our business operations in China, as well as the steps we will take to protect human rights with respect to those operations.

Verizon does not provide consumer or residential Internet access services in China¹, nor does Verizon offer email, search, hosting, VoIP, chat, social-networking, or other more traditional Internet service provider (ISP) services to Chinese subscribers. In that regard, our business activities in China are quite different from some of the consumer-oriented services we understand are offered by companies such as Microsoft, Yahoo, and Google.

Verizon does maintain business operations in China that provide various services to business customers, including Chinese branch offices of global multinational corporations. Verizon maintains a formal legal presence in China through a wholly foreign owned enterprise ("WFOE"), with offices and employees in Beijing, Shanghai, and Guangzhou. Because the overall Chinese communications licensing regime provides limited market access to foreign-owned companies, Verizon's WFOE is not licensed to provide communications services to customers in China. Our WFOE does provide non-communications services in China which include professional services, consulting, equipment and related support services.

In addition, Verizon has implemented arrangements from outside China that enable services for business customer locations in China. These arrangements include capacity on undersea cable systems serving China and arrangements with licensed telecommunications providers in China that enable a variety of network-based communications services (e.g., private line, virtual-private-network, and other network services) for Verizon's business customer locations in China (e.g., branch offices of multi-national corporations). The market for such services is highly competitive, and Verizon competes against AT&T, British Telecom, Orange Business Services, and other local and global providers of business communications services in China.

As Verizon conducts business in China and elsewhere, we act in accordance with our Human Rights Statement and other policies concerning the privacy of our customers, as indicated above. As a business with a local presence in China and many other foreign countries, we must comply with licensing and other valid legal obligations that foreign governments impose, just as we do in the United States. While we think it less likely that a company operating under a business model such as ours would encounter human rights

¹ This letter does not address Verizon operations in Hong Kong.

The Honorable Richard J. Durbin
February 19, 2010

Page Three

issues of the type that other companies operating in China have encountered, if we were to confront allegations of human rights abuses involving our network and services, we would take such allegations very seriously and act on them promptly, consistent with our Human Rights Statement and guided by our policies on corporate responsibility. Such action may include seeking assistance or consultation, as appropriate, with pertinent U.S. government agencies.

- Comments on the Global Network Initiative (GNI). You also inquired whether Verizon attended the September 10, 2009 Open House on the GNI and whether we plan to participate in the GNI workstream.

Verizon did attend the Open House, and we have also attended other briefings and events organized by the GNI and its participants. While we applaud the objectives of the GNI to address important issues surrounding global Internet freedom, the GNI provides but one approach to these important issues. It is tailored to one segment of the Internet industry and may well have application in the context of the three GNI sponsoring companies, but we continue to find it problematic for the reasons set forth in my August 27, 2009 letter to you. At this time we are reviewing whether participation in the GNI workstream *per se* is the most productive path toward broader industry engagement. In any event, we plan to continue to monitor the efforts underway through the GNI, and hope to benefit from learning about sound practices highlighted or developed in that context. In addition, we believe various other opportunities to exchange experiences through industry and other expert organizations are also valuable and needed, and some of these efforts are already underway. For example, the US Council for International Business and the International Chamber of Commerce are engaged in ongoing work around business and human rights.

As industry participants, stakeholders, and policymakers consider the GNI and additional approaches to addressing these important issues, it is important to recognize a range of approaches that reflect the diversity of different business models of the companies that make up the Internet ecosystem and thus help to achieve broad engagement. We also look forward to working with the Global Internet Freedom Task Force at the Department of State on ways to expand the global Internet to the 5 billion people around the world who are not currently connected and to support the free flow of information across that global system.

Thank you for this opportunity to share our perspective.

Sincerely,



Kathryn C. Brown
Sr. Vice President
Public Policy Development &
Corporate Responsibility

Vittorio Colao
Group Chief Executive



19 February 2010

Senator Richard J Durbin
United States Senate
Washington
DC 20510
USA

Dear Senator Durbin,

Thank you for your letter of 29 January. We have been following the situation in China closely.

As I set out in my letter of 27 August 2009 (attached), we take our responsibilities in relation to the privacy of our customers extremely seriously and continue to strengthen our policies, practices and governance of this area. We regularly review our position and have recently established a senior management committee to ensure we monitor and address public concern relating to all aspects of our internet activities.

In relation to China, our Annual Report and Accounts disclose our 3.2% investment in China Mobile Limited, which is listed on the New York and Hong Kong stock exchanges and incorporated under the laws of Hong Kong. China Mobile Communications Corporation, a company incorporated in China, is the majority owner in China Mobile Limited through intermediate holding companies. China Mobile is a telecommunications network operator. Through our minority shareholding we hold one non-executive position on the Board. In addition, in common with many international businesses, we source significant volumes of goods and services from Chinese suppliers, and have established a sourcing centre in the country to facilitate this. This is unconnected to our holding in China Mobile Limited. We continually monitor human rights risks across all our local markets and, to the extent possible, along our supply chain. China is no exception.

In my letter of August 2009 I explained our involvement to the GNI process, in which we have invested significant time and resources. We did not participate in the GNI open house but we remain in contact with the bodies facilitating the process and monitor progress with interest. We do not rule out further engagement in the future. We remain committed to transparency on these issues and report on our positioning through our Annual Corporate Responsibility Report and our website, both of which contain further information on our initiatives in the privacy and human rights areas.

Yours sincerely,

Vittorio Colao

Vodafone Group Plc

Vodafone House, The Connection, Newbury, Berkshire RG14 2FN, England
Telephone: +44 (1635) 664 194, Facsimile: +44 (0)1635 238 000

Registered Office: Vodafone House, The Connection, Newbury, Berkshire RG14 2FN, England. Registered in England No. 1833879



Websense, Inc.
10240 Serrano Valley Road
San Diego, CA 92121

tel +1 858.320.8000
fax +1 858.458.2950

www.websense.com

February 17, 2010

Sen. Richard J. Durbin
United States Senate
Washington, DC, 20510

Re: Websense Policy on Government-Imposed Internet Censorship

To Senator Durbin:

I am writing in response to your letter to me dated January 29, 2010. Your letter sought additional information regarding Websense's policy on government-imposed Internet censorship and our corporate activities in China. You asked the following:

Please provide a detailed description of your company's business in China

Websense operates a software research and development facility in Beijing, and sells Websense web security and messaging security products in China, comprising a nominal portion of Websense's worldwide sales (less than 1/4 of one percent of Websense's worldwide sales). Websense products in China are sold to businesses and other non-governmental entities and, to the best of our knowledge, are not used to censor or restrict consumer access to the Internet.

What are our company's future plans for protecting human rights, including freedom of expression and privacy, in China?

Websense has a long-standing anti-censorship policy that is applied on a worldwide basis, including China, and is published on our Web site:

"Websense does not sell to governments or Internet Service Providers (ISPs) that are engaged in government-imposed censorship. Government-mandated censorship projects will not be engaged by Websense. If Websense does win business and later discovers that it is being used by the government, or by ISPs based on government rule, to engage in censorship of the Web and Web content, we will remove our technology and capabilities from the project.

Websense does, however, allow its products and technology to be used in 'global filtering' projects where the government mandated policy (1) prohibits minors from accessing pornography and/or (2) prohibits child pornography. With the above guidelines in place, an example of an acceptable use would be government-mandated blocking of pornography to minors by the ISP. If the government requires ISPs to block adult content from all users, but permits an adult user to gain access to that content after providing proof of age, this would be in compliance with our stated policy. Websense, however, does not engage in any arrangements with foreign governments (or government-imposed arrangements) that could be viewed as oppressive of rights."

From time to time we are notified of possible non-compliance with our policy by governmental entities or by quasi-public or private entities based on government restriction. In past situations, we have investigated and taken remedial action when appropriate. In several instances, the appropriate action was to immediately terminate the violator's access to our product. As we communicated to your staff several months ago, during 2009 we learned that two ISPs in Yemen were using our solutions in violation of our policy, and we unilaterally terminated the Yemeni ISPs' subscriptions to our products.

While we have not been informed of any misuse of our products in China, we would follow the same procedure to assess and remediate any issues. If we became aware of any misuse (or any allegations of misuse), we would challenge the customer to understand how our product is being used, as well as conduct independent testing to validate that use. Because our product is reliant on daily updates to our url database, if we determine that our product is being abused, we can block all database updates to a customer. This provides us with a relatively unique ability, in a very short period of time, to render our software worthless for the transgressing customer.

Our complete review policy, which is posted on our Web site, states:

"While Websense strives to permit our customers to configure their web, data and messaging use policies in whatever manner they desire, Websense reserves the right to investigate unauthorized or improper use of Websense products. In the event that product use is determined to be contrary to Websense's product terms and conditions and/or our corporate policies, appropriate measures will be taken.

When Websense receives a complaint or other information pertaining to alleged improper use of our products, we seek to initially identify (1) the customer who has allegedly used our products improperly, (2) the specific product involved, and (3) the alleged improper use. The matter is referred to our Legal Department, who then investigates the possible inappropriate use, contacting relevant members of the Websense team, our channel partners, and ultimately, our customer.

We gather information to determine whether or not the claim of alleged improper use is reasonably credible. This can often be difficult because Websense does not have visibility into the web, data and messaging enforcement policies implemented by our customers. Once we reasonably believe that a violation may have occurred, we contact the customer. Typically, we explain to the customer what they must do to come into compliance, with the hope that they will make the appropriate changes. Dialogue with the relevant customer usually resolves the issue.

However, if inappropriate use is determined to have occurred, and open discussion does not resolve the issue, Websense will take any one or more of the following actions which may include but is not limited to the following:

- Verbal or written warnings.
- Bill the customer for any charges related to the improper use.

- Notify the customer that their product subscription will be suspended or terminated if the customer cannot (a) provide proof of compliance with Websense terms, conditions and policies, or (b) commit to comply with Websense terms, conditions and policies.
- If the customer does not provide (a) or (b) above within a reasonable time following notice of suspension or termination from Websense, suspend or terminate the customer's product subscription.
- Initiate legal action."

Did representatives of our company attend the GNI open house?

Yes, Websense participated in the GNI open house.

Does our company plan to participate in the GNI workstream?

Websense is extremely supportive of the philosophies underlying the Global Network Initiative, as demonstrated by Websense's independently developed policy against government-imposed censorship. In fact, several Websense competitors actively pursue financially lucrative business arrangements with governments that use their software to filter consumer Internet access, and Websense has voluntarily chosen to concede that business to our competition. We believe the GNI can make a difference in raising social awareness of the human rights issues and hopefully garner more widespread support in the industry.

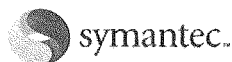
We are concerned, however, with the administrative costs imposed by the GNI in the current economic climate. The GNI's initial \$200,000 commitment over two years is significant for a company of Websense's size, and the continuing independent third-party compliance audit for GNI implementation guidelines is costly both in terms of dollars and employee resources. If the \$200,000 up front fee was waived, Websense would join the GNI. Websense would like to see the companies with the greatest resources, and whose practices regarding censorship are most questionable, take the economic lead.

If you have any further questions, please let me know.

Regards,



Gene Hodges
Chief Executive Officer
Websense, Inc.



March 5, 2010

The Honorable Richard J. Durbin, Chairman
U.S. Senate Committee on the Judiciary
Subcommittee on Human Rights and the Law
United States Senate
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Durbin:

Thank you for your follow-up letter dated January 29, 2010 requesting further information on Symantec's human rights policy. Since my initial response to you on January 15, 2010, we continue to perform our internal due diligence in considering your recommendation that Symantec participate in the Global Network Initiative (GNI).

At Symantec we take human rights seriously. After a rigorous internal review process, Symantec became a signatory the UN Global Compact (UNGC) on March 14, 2006. The UNGC sets forth a set of ten principles focused on human rights, labor, environment and anti-corruption. In fact, we were one of the first software companies to sign on to this important initiative.

Per your request, we are exploring participation in the Global Network Initiative (GNI). Since my recent letter to you we have been performing our due diligence including the following actions:

- Symantec is on the GNI working group distribution list
- We have formed an internal committee to conduct our own due diligence around this issue. This committee is headed by our General Counsel Scott Taylor, and includes members from government affairs, ethics and compliance, privacy and corporate social responsibility.
- We recently held an informational meeting with Dunstan Hope, who represents Business for Social Responsibility (BSR) and acting in the capacity of facilitator for the GNI and Chuck Cosson, Senior Policy Council for Microsoft.

Symantec Corporation 350 Ellis Street, Mountain View, CA 94043 telephone (650) 527 8000 fax (650) 527 2908 www.symantec.com

- On March 4th we participated in a State Department meeting on Internet Freedom led by Undersecretaries Maria Otero and Robert Hormats.
- We are also initiating discussions with the Center for Democracy and Technology (CDT), one of the leaders of the GNI effort.

We understand that GNI addresses some unique privacy questions and access to information aspects to the human rights dialogue. We believe that GNI is worthy of consideration and want to assure you that we're making every effort to learn more about GNI and if there is a strategic role for these principles with respect to our overall human rights policy as a company.

As the world's information security leader, Symantec follows a rigorous privacy policy¹ to protect our customers' information. Our business policies are closely monitored and aligned with our industry leading human rights policy. Our technology is used to protect our customer's information. Our philosophy is that the protection of our customer comes first regardless of geography or the government's political philosophy of where that customer resides.

Your letter of January 29 also asked about our operations in China. Like many other multi-national corporations Symantec does business in China, including product development, and sales. Specific activities include: Sales and development centers located in Chengdu, Beijing, Hong Kong, Shanghai, Guangzhou and Shenzhen, and a joint venture with networking manufacturer Huawei Technologies Co. where we are the minority partner.

Symantec is committed to respecting human rights where we do business around the globe, including in China. Thank you again for your interest in this important topic of freedom and human rights. Be assured that Symantec will continue to abide by high standards of corporate responsibility, including human rights as we conduct business throughout the world.

Regards,



Enrique Salem

¹ Your Privacy Rights. <http://www.symantec.com/about/profile/policies/privacy.jsp>

HBC 3COM TippingPoint

Neal D. Goldman
Executive Vice President
Chief Administrative and Legal Officer

3Com Corporation
350 Campus Drive
Marlborough, MA 01752
T: 508.323.1010
F: 508.323.1044
E: neal_goldman@3com.com

www.3com.com

3COM

Neal Goldman
3Com Corporation
350 Campus Drive
Marlborough, MA 01752

Senator Richard J. Durbin
United States Senate
309 Harte Senate Office Building
Washington, DC 20510

3COM

Neal Goldman
3Com Corporation
350 Campus Drive
Marlborough, MA 01752

Senator Tom Coburn
United States Senate
172 Russell Senate Office Building
Washington, DC 20510

August 12, 2009

Senator Richard J. Durbin
Senator Tom Coburn
United States Senate
Washington, DC 20510

Dear Senators Durbin and Coburn:

I am responding to your letter dated August 6, 2009 addressed to our Chief Executive Officer, Robert Mao. Mr. Mao has asked me to respond on behalf of our Company since my regular duties include government relations.

First, I apologize for the confusion regarding your previous contact with our Company. Your August 6, 2009 letter is the first we heard of your desire to have Mr. Mao meet with staff from the Human Rights and Law Sub Committee. Had we been aware of this request, we would have met with your representatives. Please be assured that it is always our policy to fully cooperate in such matters.

Before I respond to your specific questions, I would like to explain a bit about 3Com's business. 3Com provides data networking infrastructure products. Our products are primarily switches, routers and in-line security products that help organizations manage the flow of data through computers and systems. We do not provide user interface products similar to Google, Yahoo or Microsoft. Our products do not sit on a user's desk, and they are not used to directly access the internet. Therefore, we believe that 3Com is in a very different segment of the information and communications technology sector ("ICT") than the companies referenced in your letter such as Microsoft, Google and Yahoo. While those companies interface directly with individuals and act as a primary interface for them to access the internet, we do not.

HC 3COM TippingPoint
August 12, 2009
Page 2

Because this communication comes to us without our having had the opportunity to meet with your representatives and better understand the issues raised, we would like to more fully engage before responding to your specific questions. Although we have, of course, stayed current on the reported actions of certain countries to control internet access, we were not aware of the GNI initiatives. We are now researching the issue more fully and talking to our colleagues in other companies. I would be happy to meet with your representatives at their convenience as an important step in our engagement on this issue.

Please be assured that 3Com values individual freedom and we believe our products can be used to facilitate broad access to information on a global basis.

I would be happy to discuss this further with your office representatives.

Very truly yours,



Neal D. Goldman
Executive Vice President
Chief Administrative and Legal Officer

NDG/ljt
Cc: Robert Mao, CEO

03/23/2010 20:31 5083231502

EMASRI FAX

PAGE 01/01



Robert Mao
Chief Executive Officer

3Com Corporation
350 Campus Drive
Marlborough, MA 01752-3044
T: 508.323.1371
F: 508.323.1502
E: rob_mao@3com.com
www.3com.com

March 22, 2010

Senator Richard Durbin
309 Hart Senate Building
Washington, DC 20510

Dear Senator Durbin,

Thank you for your letter dated January 29, 2010. In that letter, you asked for additional responses to the answers we provided to your letter dated August 6, 2009. I would like to point out to you that in November, 2009, Hewlett Packard and 3Com entered into a definitive merger agreement. It is our expectation that the merger will close in April, 2010 and at that time, 3Com will operate as a business unit of Hewlett Packard. Once the deal closes, the current Board of Directors will change and I will no longer be the CEO of 3Com. With a major structural change planned to take place in the very near term, I am reluctant to make commitments about 3Com's plans. In view of the pending merger agreement, I suggest that we table this matter for a couple of months and allow Hewlett Packard to address your questions.

Very truly yours,

Robert Mao
Chief Executive Officer
3Com Corporation

RYLM/ljt

03/24/2010 8:34AM



August 27, 2009

The Honorable Richard J. Durbin
Chairman
Subcommittee on Human Rights and the Law
United States Senate
Washington, DC 20510

The Honorable Tom Coburn
Ranking Member
Subcommittee on Human Rights and the Law
United States Senate
Washington, DC 20510

Dear Chairman Durbin and Ranking Member Coburn:

Thank you for your letter of August 6th concerning Apple's approach to addressing human rights issues where we conduct business around the world. Apple appreciates your long-standing efforts to encourage technology companies to establish policies and procedures to address the potential for human rights violations, such as those contemplated by the principles advocated under the recently formed Global Network Initiative (GNI).

Apple shares GNI's objective in support of individual freedom of expression and privacy in adherence to universally held standards for human rights. Internally, Apple has already implemented a comprehensive and principled approach to address human rights around the world. And, as a company known for its ardent focus on delivering innovative and award winning hardware and software products, Apple also remains strongly committed to ensuring that appropriate operational codes of conduct are followed and maintained throughout our global operations.

As you may know, Apple's worldwide product offerings consist of hardware, such as computers, iPods, and iPhones, and software, such as Mac OS X and the iLife suite (which includes iTunes, iPhoto, iMovie, iDVD, and Garageband). While these products all access networks, Apple neither operates nor directly manages any of the networks that these products can access. The iPhone, for example, currently operates in 81 countries and in these markets, Apple has agreements with various carriers to provide our iPhone users with mobile network access. But our relationship with the users involves the devices themselves and not the networks upon which they can operate, which appears to be the primary focus of the GNI.

Apple
1 Infinite Loop
Cupertino, CA 95014
408.996.4600
apple.com
www.apple.com



As a non-network operator and a non-ISP, we have focused on upholding internationally recognized human rights in the area where we can make a difference, which is through our contractual relationships with our third-party original equipment manufacturing (OEM) partners and our suppliers. Apple is strongly committed to ensuring the highest standards of social responsibility wherever our products are made. Apple requires our suppliers to provide safe working conditions, to treat employees fairly by upholding human rights and treating them with dignity and respect, and to use environmentally responsible manufacturing processes.

Apple is an active participant in the Electronic Industry Citizenship Coalition (EICC), a group of companies in the electronic industry working together to improve social responsibility in the global supply chain. Apple's Supplier Code of Conduct is modeled on and contains language from the EICC Code of Conduct. In addition, we used internationally recognized standards from the International Labour Organization (ILO), the Universal Declaration of Human Rights (UDHR), Social Accountability International (SAI), and the Ethical Trading Initiative (ETI) to guide us in preparing our Code and implementing our operational procedures for administering it. Our Supplier Code of Conduct can be downloaded at our supplier responsibility website www.apple.com/supplierresponsibility and has been attached to this letter.

To ensure that our Supplier Code requirements are followed, Apple undertakes comprehensive and rigorous onsite audits of our third party suppliers and their facilities. These audits are supported by in-region staff and third-party experts who know the language and understand local regulations and practices. Should corrective actions be required, plans are developed and corrective actions are taken not only to address specific and potential violations, but to also ensure that management systems are in place to prevent reoccurrence. While most findings can be corrected immediately, our team tracks completion of each corrective action and performs a Corrective Action Verification audit to confirm that the supplier continues to meet our requirements. The results of our audits are made public and detailed reports are available on our supplier responsibility website.

Apple is also currently working closely with our U.S. based tech industry colleagues under the auspices of the Information Technology Industry Council (ITI) to share our own best practices and to express our common objectives for protecting individual privacy and ensuring that human rights are respected.

Apple shares your belief that global technology companies should take reasonable steps to effectively protect human rights. The voluntary objectives and principles set forth by the GNI would appear to serve well certain segments of the technology



community, particularly Internet Service Providers and Network Operators. As a non-network operator or ISP, we believe that there is more than one approach to meet this shared goal. As we have explained, we have instituted a rigorous program within Apple for protecting human rights of which we are proud, and we remain committed to working closely with our technology industry colleagues at ITI to develop common principles in this regard.

We appreciate your commitment to protecting individual freedom of expression and protecting human rights, and for allowing us to educate you on our fervent commitment to the same.

Sincerely,

A handwritten signature in dark ink, appearing to read "Daniel Cooperman", is written over a light gray horizontal line.

Daniel Cooperman
Senior Vice President
General Counsel & Secretary

Apple Supplier Code of Conduct

Apple is committed to ensuring that working conditions in Apple's supply chain are safe, that workers are treated with respect and dignity, and that manufacturing processes are environmentally responsible. Apple's suppliers ("Suppliers") are obligated, in all of their activities, to operate in full compliance with the laws, rules, and regulations of the countries in which they operate. This Supplier Code of Conduct ("Code") goes further, drawing upon internationally recognized standards, in order to advance social and environmental responsibility. Apple requires that Suppliers implement this Code using the management systems described below.

The Apple Supplier Code of Conduct is modeled on and contains language from the Electronic Industry Code of Conduct. Recognized standards such as International Labour Organization Standards (ILO), Universal Declaration of Human Rights (UDHR), Social Accountability International (SAI), and the Ethical Trading Initiative (ETI) were used as references in preparing this Code and may be useful sources of additional information. A complete list of references is provided at the end of this Code. As an extension of the Code, Apple maintains a series of detailed Standards that clarify our expectations for compliance.

Labor and Human Rights

Suppliers must uphold the human rights of workers, and treat them with dignity and respect as understood by the international community.

Antidiscrimination

Suppliers shall not discriminate against any worker based on race, color, age, gender, sexual orientation, ethnicity, disability, religion, political affiliation, union membership, national origin, or marital status in hiring and employment practices such as applications for employment, promotions, rewards, access to training, job assignments, wages, benefits, discipline, and termination. Suppliers shall not require a pregnancy test or discriminate against pregnant workers except where required by applicable laws or regulations or prudent for workplace safety. In addition, Suppliers shall not require workers or potential workers to undergo medical tests that could be used in a discriminatory way except where required by applicable law or regulation or prudent for workplace safety.

Fair Treatment

Suppliers must be committed to a workplace free of harassment. Suppliers shall not threaten workers with or subject them to harsh or inhumane treatment, including sexual harassment, sexual abuse, corporal punishment, mental coercion, physical coercion, verbal abuse or unreasonable restrictions on entering or exiting company provided facilities.

Prevention of Involuntary Labor

Suppliers shall not use any form of forced, bonded, indentured, or prison labor. All work must be voluntary and workers shall be free to leave work or terminate their employment with reasonable notice. Workers must not be required to surrender any government-issued identification, passports, or work permits as a condition of employment. Suppliers shall ensure that third party labor agencies providing workers are compliant with the provisions of the Code and sending country and receiving country laws, whichever is more stringent in its protection of workers. Suppliers shall ensure that contracts for both direct and contract workers clearly convey the conditions of employment in a language understood by the worker. Suppliers shall be responsible for payment of all fees and expenses in excess of the amount equal to one month of the worker's anticipated net wages. Such fees and expenses include, but are not limited to expenses associated with recruitment, processing or placement of both direct and contract Workers.

Prevention of Under Age Labor

Child labor is strictly prohibited. Suppliers shall not employ children. The minimum age for employment or work shall be 15 years of age, the minimum age for employment in that country, or the age for completing compulsory education in that country, whichever is higher. This Code does not prohibit participation in legitimate workplace apprenticeship programs that are consistent with Article 6 of ILO Minimum Age Convention No. 138 or light work consistent with Article 7 of ILO Minimum Age Convention No. 138.

Juvenile Labor

Suppliers may employ juveniles who are older than the applicable legal minimum age for employment but are younger than 18 years of age, provided they do not perform work likely to jeopardize their health, safety, or morals, consistent with ILO Minimum Age Convention No. 138.

Working Hours

Except in Emergency or Unusual Situations, a workweek shall be restricted to 60 hours, including overtime, workers shall be allowed at least one day off every seven-days, and overtime shall be voluntary. Under no circumstances will workweeks exceed the maximum permitted under applicable laws and regulations. Suppliers must offer vacation time, leave periods, and holidays consistent with applicable laws and regulations.

Wages and Benefits

Suppliers must pay all workers at least the minimum wage required by applicable laws and regulations and provide all legally mandated benefits. In addition to their compensation for regular hours of work, workers must be compensated for overtime hours at the premium rate required by applicable laws and regulations. Suppliers shall not use deductions from wages as a disciplinary measure. Workers must be paid in a timely manner, and the basis on which workers are being paid must be clearly conveyed to them in a timely manner.

Freedom of Association

Suppliers must respect the right of workers to associate freely, form and join workers organizations of their own choosing, seek representation, and bargain collectively, as permitted by and in accordance with applicable laws and regulations. Suppliers shall not discriminate with respect to employment based on union membership and, in particular, shall not make employment subject to the condition that the worker relinquish union membership or agree not to join a union or cause the dismissal of or otherwise prejudice a worker by reason of union membership or participation in union activities outside working hours (or within working hours if the Supplier has consented to such activities or if required by applicable law or regulation). Suppliers must protect against acts of interference with the establishment, functioning, or administration of workers' organizations in accordance with applicable laws and regulations.

Health and Safety

Apple recognizes that integrating sound health and safety management practices into all aspects of business is essential to maintain high morale and produce innovative products. Suppliers must be committed to creating safe working conditions and a healthy work environment for all of their workers.

Occupational Injury Prevention

Suppliers must eliminate physical hazards where possible. Where physical hazards cannot be eliminated, Suppliers must provide appropriate engineering controls such as physical guards, interlocks, and barriers. Where appropriate engineering controls are not possible, Suppliers must establish appropriate administrative controls such as safe work procedures. In all cases, Suppliers must provide workers appropriate personal protective equipment. Workers must have the right to

refuse unsafe working conditions without fear of reprisal until management adequately addresses their concerns.

Prevention of Chemical Exposure

Suppliers must identify, evaluate, and control worker exposure to hazardous chemical, biological, and physical agents. Suppliers must eliminate chemical hazards where possible. Where chemical hazards cannot be eliminated, Suppliers must provide appropriate engineering controls such as closed systems and ventilation. Where appropriate engineering controls are not possible, Suppliers must establish appropriate administrative controls such as safe work procedures. In all cases, Suppliers must provide workers appropriate personal protective equipment.

Emergency Prevention, Preparedness, and Response

Suppliers must anticipate, identify, and assess emergency situations and events and minimize their impact by implementing emergency plans and response procedures, including emergency reporting, worker notification and evacuation procedures, worker training and drills, appropriate first-aid supplies, appropriate fire detection and suppression equipment, adequate exit facilities, and recovery plans.

Occupational Safety Procedures and Systems

Suppliers must establish procedures and systems to manage, track, and report occupational injury and illness. Such procedures and systems should encourage worker reporting, classify and record injury and illness cases, investigate cases and implement corrective actions to eliminate their causes, provide necessary medical treatment, and facilitate the workers' return to work.

Ergonomics

Suppliers must identify, evaluate, and control worker exposure to physically demanding tasks, including manual material handling, heavy lifting, prolonged standing, and highly repetitive or forceful assembly tasks.

Dormitory and Dining

Suppliers must provide workers with clean toilet facilities, access to potable water, and sanitary food preparation and storage facilities. Worker dormitories provided by the Supplier or a labor agent must be clean and safe and provide adequate emergency egress, adequate heat and ventilation, reasonable personal space, and reasonable entry and exit privileges.

Communication

In order to foster a safe work environment, Suppliers shall ensure that workers receive appropriate workplace health and safety information and training, including written health and safety information and warnings in the primary language of its workers. Suppliers must post Material Safety Data Sheets in the primary language of its workers for any hazardous or toxic substances used in the workplace and properly train workers who will come into contact with such substances in the workplace.

Worker Health and Safety Committees

Suppliers are encouraged to initiate and support worker health and safety committees to enhance ongoing health and safety education and to encourage worker input regarding health and safety issues in the workplace.

The Environment

At Apple, environmental considerations are an integral part of our business practices. Suppliers must be committed to reducing the environmental impact of their designs, manufacturing processes, and waste emissions.

Hazardous Substance Management and Restrictions

Suppliers must comply with the most recent version of Apple's Regulated Substances Specification,

069-0135 and with any applicable laws and regulations prohibiting or restricting specific substances. To ensure safe handling, movement, storage, recycling, reuse, and disposal, Suppliers must identify and manage substances that pose a hazard if released to the environment and comply with applicable labeling laws and regulations for recycling and disposal.

Wastewater and Solid Waste Emissions

Wastewater and solid waste generated from operations, industrial processes, and sanitation facilities must be monitored, controlled, and treated as required by applicable laws and regulations before discharge or disposal.

Air Emissions

Air emissions of volatile organic chemicals, aerosols, corrosives, particulates, ozone depleting chemicals, and combustion by-products generated from operations must be characterized, monitored, controlled, and treated as required by applicable laws and regulations before discharge.

Environmental Permits and Reporting

Suppliers must obtain, maintain, and keep current all required environmental permits (e.g. discharge monitoring) and registrations and follow the operational and reporting requirements of such permits.

Pollution Prevention and Resource Reduction

Suppliers must endeavor to reduce or eliminate waste of all types, including water and energy, by implementing appropriate conservation measures in their facilities, in their maintenance and production processes, and by recycling, re-using, or substituting materials.

Ethics

Suppliers must be committed to the highest standards of ethical conduct when dealing with workers, suppliers, and customers.

Corruption, Extortion, or Embezzlement

Corruption, extortion, and embezzlement, in any form, are strictly prohibited. Suppliers shall not engage in corruption, extortion or embezzlement in any form and violations of this prohibition may result in immediate termination as an Apple Supplier and in legal action.

Disclosure of Information

Suppliers must disclose information regarding its business activities, structure, financial situation, and performance in accordance with applicable laws and regulations and prevailing industry practices.

No Improper Advantage

Suppliers shall not offer or accept bribes or other means of obtaining undue or improper advantage.

Fair Business, Advertising, and Competition

Suppliers must uphold fair business standards in advertising, sales, and competition.

Whistleblower Protection and Anonymous Complaints

Suppliers must create programs to ensure the protection of Supplier and worker whistleblower confidentiality and prohibit retaliation against workers who participate in such programs in good faith or refuse an order that is in violation of the Apple Supplier Code of Conduct. Suppliers shall provide an anonymous complaint mechanism for workers to report workplace grievances in accordance with local laws and regulations.

Community Engagement

Suppliers are encouraged to engage the community to help foster social and economic development and to contribute to the sustainability of the communities in which they operate.

Protection of Intellectual Property

Suppliers must respect intellectual property rights; safeguard customer information; and transfer of technology and know-how must be done in a manner that protects intellectual property rights.

Management Systems

Suppliers must adopt or establish a management system designed to ensure compliance with this Code and applicable laws and regulations, identify and mitigate related operational risks, and facilitate continuous improvement. ISO 14001, OHSAS 18001, Eco Management and Audit System (EMAS) may be useful resources. The management system should contain the following elements:

Company Commitment

A corporate social and environmental responsibility statement affirming the Supplier's commitment to compliance and continual improvement, to be posted in the primary local language at all of the Supplier's worksites.

Management Accountability and Responsibility

Clearly identified company representatives responsible for ensuring implementation and periodic review of the status of the Supplier's management systems.

Legal and Customer Requirements

A process to identify, monitor, and understand applicable laws and regulations and the additional requirements imposed by this Code. Supplier shall obtain, maintain and keep current a valid business license as required by applicable laws and regulations.

Risk Assessment and Management

A process to identify environmental, health and safety, business ethics, labor, human rights and legal compliance risks associated with their operations, determine the relative significance of each risk, and implement appropriate procedures and physical controls to ensure compliance and control the identified risks. Risk assessments for health and safety must include warehouse and storage facilities, plant and facility support equipment, laboratories and test areas, bathrooms, kitchens, cafeterias, and worker housing.

Performance Objectives with Implementation Plans and Measures

Written standards, performance objectives, targets, and implementation plans, including a periodic assessment of the Supplier's performance against those objectives.

Training

Programs for training managers and workers to implement the Supplier's policies, procedures, and improvement objectives.

Communication

A process for communicating clear and accurate information about the Supplier's performance, practices, and expectations to its workers, Suppliers, and customers.

Worker Feedback and Participation

An ongoing process to obtain feedback on processes and practices related to this Code and to foster continuous improvement.

Audits and Assessments

Periodic self-evaluations to ensure that the Supplier, its subcontractors and its next-tier Suppliers are complying with this Code and with applicable laws and regulations. Apple may visit (and/or have external monitors visit) Supplier facilities, with or without notice, to assess compliance with this Code and to audit Supplier's wage, hour, payroll, and other worker records and practices.

Corrective Action Process

A process for timely correction of any deficiencies identified by an internal or external audit, assessment, inspection, investigation, or review.

Documentation and Records

Creation of documents and records to ensure regulatory compliance and conformity to this Code, with appropriate confidentiality measures to protect privacy.

References

Apple consulted the following references in preparing this Code.

Eco Management & Audit System

www.quality.co.uk/emas.htm

Electronic Industry Code of Conduct, October 2004

www.hp.com/hpinfo/globalcitizenship/environment/pdf/supcode.pdf

Ethical Trading Initiative

www.ethicaltrade.org/

ILO Code of Practice in Safety and Health

www.ilo.org/public/english/protection/safework/cops/english/download/c000013.pdf

ILO International Labor Standards

www.ilo.org/public/english/standards/norm/whatare/fundam/index.htm

ISO 14001

www.iso.org

National Fire Protection Agency

www.nfpa.org/catalog/home/AboutNFPA/index.asp

OECD Guidelines for Multinational Enterprises

www.oecd.org

OHSAS 18001

www.bsi-global.com/index.xalter

SA 8000

www.cepa.org/

SAI

www.sai-intl.org

United Nations Convention Against Corruption

www.unodc.org/unodc/en/crime_convention_corruption.html

United Nations Global Compact

www.unglobalcompact.org

Universal Declaration of Human Rights

www.un.org/Overview/rights.html

UN Norms on the Responsibilities of Transnational Corporations and other Business Enterprises with Regard to Human Rights

www.ohchr.org

This Code is not intended to create new or additional rights for any third party.

Version 3.1. Copyright © 2009 Apple Inc. All rights reserved.



Timothy P. McKone
Executive Vice President
Federal Relations

AT&T Services, Inc.
1133 21st Street, NW
Suite 900
Washington, DC 20036

T: 202.463.4144
F: 202.463.4183
tm3703@att.com

August 25, 2009

Hon. Richard J. Durbin
United States Senate
309 Hart Senate Office Building
Washington, DC 20510

Hon. Tom Coburn
United States Senate
172 Russell Senate Office Building
Washington, DC 20510

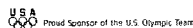
Dear Senators Durbin and Coburn:

I am responding to your letter dated August 6, 2009, to our Chairman and CEO, Randall Stephenson, regarding the Global Network Initiative ("GNI").

AT&T shares your goal of furthering free and full communication throughout the world, and is proud to be at the forefront of creating the opportunities for human interaction that you seek to protect and expand; indeed, it is the essence of our business. Among other things, we have worked with over 400 foreign carriers in over 220 countries and territories, including many emerging markets, to connect people and institutions around the globe. Now, countries that, until recently, had only a handful of international voice circuits enjoy millions of international voice, data and Internet connections. In our view, then, the most important step that we can take is to continue these substantial investments; they constitute an important pillar of advancing human engagement and free speech.

At the same time, we are mindful that government action can stifle freedom of expression. For this reason, we take quite seriously our role in ensuring that government requests that could have the effect of limiting free speech or invading our customers' privacy undergo rigorous evaluation. At a minimum, when we receive a directive from a foreign government or agency to, for instance, block access to certain content or websites, we confirm that the request is authorized under local law; authenticate both that the request conforms with applicable rules and that the requesting person or institution is, indeed, authorized to submit the request; seek as much specificity as possible regarding the nature of the request; and, if the request is lawful and properly authorized, tailor our compliance with it as narrowly as possible. Moreover, we employ technological means to ensure that the ultimate effects of any mandated restraints on communication or access to information are as limited in scope as possible.¹

¹ In this regard, it is worth noting that, with respect to its direct provision of service in foreign countries, AT&T mostly provides enterprise-based services to larger business customers; that is, our international business is not at this time built primarily to serve mass market customers. Given this business-focused customer base, AT&T encounters relatively fewer requests or inquiries that might raise the specter of censorship or privacy violations as compared to other American companies in the Information and Communications Technology ("ICT") sector that have a more mass-market focus.



Senator Richard J. Durbin
Senator Tom Coburn
August 25, 2009
Page 2

We also recognize that there is an important role for governments, voluntary organizations and other institutions to play in promoting freedom of expression. One of many such voluntary associations is GNI, which focuses on the role of the ICT sector in protecting freedom of expression and privacy rights. While AT&T has had productive discussions with GNI members and continues to follow the initiative's progress, AT&T has not joined GNI, nor have we identified a specific set of criteria or thresholds that would have to be met in order for AT&T to consider joining GNI.

While there is nothing necessarily assailable in the foundation of GNI's Principles, which relate to broad notions of freedom of expression and privacy, it is difficult, based on the facts known to date, to foresee their practical implementation. Indeed, it is not clear to us that GNI's Governance, Accountability and Learning Framework, or its Implementation Guidelines, apply well to the business of a network provider. AT&T enables global connectivity, in part, by maintaining a variety of supply and correspondent relationships with foreign carriers, including many foreign-government-owned carriers, in nearly every country and territory around the world. As such, AT&T must be particularly careful about accepting an obligation that might make it responsible for the actions or policies of such foreign carriers. This is generally not a material concern for GNI members like Google and Yahoo!, which are not in the business of providing global communications capability and therefore do not necessarily have to establish direct bilateral relationships with foreign carriers – over whom they will be able ultimately to exercise little or no control – in order to offer service.

Moreover, the Implementation Guidelines do not, as crafted, appear sufficiently flexible to address the full range of unforeseen events and situations that might arise. Likewise, AT&T has concerns that the record keeping and audit and reporting elements of the Framework and Guidelines could adversely impact customer privacy. That is, the Framework and Guidelines presage the creation of a pervasive structure for compliance with the broad Principles and for third-party evaluation of such compliance. Without the details of that structure, however, it is difficult to judge whether AT&T's membership truly would be appropriate.

Finally, we have concerns about the efficacy of certain measures, such as the expectation that GNI members will challenge another sovereign nation's laws in foreign or domestic courts. When AT&T operates in a foreign country, it is subject to the laws and regulations of that country, just like foreign-owned companies operating in the United States are subject to the laws and regulation of our country. For this reason, AT&T exercises diligent care in determining the activities we conduct in each market and establishing the practices necessary to manage our response to an authenticated government demand for legal cooperation. We take these steps because it is the right thing to do, and also because it is necessary to protect the high up front capital investment required to provide communications services around the world. But, once we make the considered decision to invest in a new market – and, in the process, foment further international interaction – we must be judicious in making any decision to challenge the validity of that nation's laws, and are reluctant to take on the obligation to do so without consideration of all the unique circumstances at hand in the particular country.

Senator Richard J. Durbin
 Senator Tom Coburn
 August 25, 2009
 Page 3

While we are not prepared to join GNI at this time, we are interested in learning, as events unfold and as GNI's framework is tested and implemented, how effective GNI is in advancing its objectives. We expect that AT&T, other interested companies, and policymakers may have a better indication of GNI's performance after evaluating initial rounds of GNI's public audit reports, and whether or not those engender positive changes or reactions.

Thank you for seeking AT&T's perspectives on these critically important matters. Please feel free to contact me should you require additional information.

Respectfully,





Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Direct: 408 526 4000
FAX: 408 526 4100
www.cisco.com

August 27, 2009

The Honorable Richard Durbin
United States Senate
Washington, DC 20510

The Honorable Tom Coburn
United States Senate
Washington, DC 20510

Dear Senators Durbin and Coburn:

Thank you for your August 6th letter addressed to John Chambers regarding Cisco's approach to human rights issues and the Global Network Initiative (GNI). I am responding to your questions in my capacity as Cisco's Chief Legal Officer.

Q1) What are your company's views on the GNI?

A1) As we understand it, the GNI was initially formed in response to concerns about the issues Internet service providers face as they are forced to comply with domestic laws and policies by governments that do not share commonly-held views of free expression and the right to privacy.

While Cisco is not an Internet service provider like current GNI participants, we believe the GNI's core principles for network operation are appropriate for those companies that are network operators. Were we to operate a network anywhere in the world, it would be our intention to act in accordance with those principles.

Q2) Will your company consider joining the GNI? If yes, please describe the process you will follow to consider joining the GNI. If no, why not?

A2) We have met with GNI principals several times to discuss the group's goals and outcomes. It was clear from those discussions that the GNI principles were heavily focused on addressing issues faced by Internet service providers. Since the business model for service providers is considerably different from that of equipment vendors like Cisco, we do not believe that the initial focus of the GNI would be relevant to how we operate. In particular, the GNI model may not be suitable for network infrastructure suppliers since there are literally dozens of companies, both U.S. and non-U.S.-based, including some based in China, which sell equipment and software for operation of the Internet around the world.

Page 2
 United States Senate
 August 27, 2009

The most fundamental issue, as illustrated by the recent Green Dam debate, is how the purchasers and end users of information and communications technology in other countries are directed to use those products by their governments, which is beyond the control of hardware vendors where functionality is generic. While we do plan to meet with GNI principals again in the coming weeks to discuss the best way for the goals of the GNI to be implemented, we believe those issues are more appropriately addressed by government efforts to drive consistency in global internet standards and by industry associations rather than by individual companies.

Q3) Does your company currently follow any of the GNI principles?

A3) Please see A1.

Q4) Please describe your company's policies and practices for advancing and protecting human rights and minimizing the risk that your products and/or services will facilitate human rights abuses.

As I noted in my testimony before the Human Rights Subcommittee in May 2008, Cisco complies with all U.S. Government regulations that 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, regarding supply of equipment for law enforcement purposes.

Since 2001, Cisco has supported the United Nations Global Compact (UNGC), which brings businesses together with UN agencies, labor organizations, civic organizations, and governments, to advance human rights principles in the areas of human rights, labor, environment, and anti-corruption. The Compact includes the following principles:

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 ideals behind the UNGC are incorporated into our core operating principles as a company.

Cisco also has basic human rights guidelines that are publicly disclosed as part of our Corporate Citizenship Report. Those guidelines support the United Nations Universal Declaration of Human Rights, and as outlined in our Code of Business Conduct and

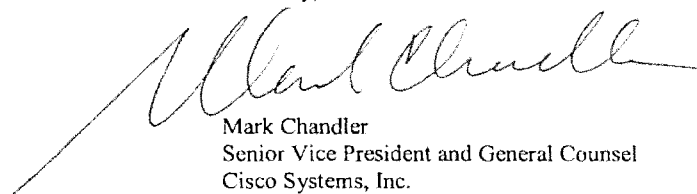
Page 3
United States Senate
August 27, 2009

employee policies, we expect all our employees to "treat others equally and with respect and dignity."

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 mandating country-specific security requirements. We do not design custom or closed Internet systems. Furthermore, unlike many other companies, we do not offer the network components to network operators which are most often singled-out for use for repression of communications, such as that which permits interception of voice communications.

Thank you for the opportunity to provide Cisco's responses to your questions on this important topic. Please let me know if you have any further questions.

Sincerely,



Mark Chandler
Senior Vice President and General Counsel
Cisco Systems, Inc.

*Dell Inc.
1225 I Street, NW, #300
Washington, DC 20005*

*Telephone: 202.408.3355
Telefax 202.408.7664
www.dell.com*



August 27, 2009

The Honorable Richard J. Durbin
U.S. Senate
309 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Tom Coburn
U.S. Senate
172 Russell Senate Office Building
Washington, D.C. 20510

Dear Senators Durbin and Coburn,

Thank you for your letter of August 6, 2009 inquiring about Dell's approach to human rights issues. As the person responsible for Dell's corporate responsibility policies, I have been asked to reply for the company. Dell is committed to protecting human rights, whether with respect to our own employees, suppliers and their workers, or customers. We are familiar with the Global Network Initiative, whose principles and guidance generally mirror Dell's own approach in this area. We also know that the Information Technology Industry Council is currently developing a list of principles designed to meet the specific needs and issues faced by the hardware industry.

Dell's Commitment to Human Rights

Dell is committed to treating our employees fairly and with dignity and respect. Our Code of Conduct sets out our commitment to workplace equality, compliance with all applicable legal requirements, and ensuring that our employees work in a safe and healthy environment.

Dell has also taken steps to help ensure that working conditions in its supply chain are safe, that workers are treated with respect and dignity, and that business operations are environmentally responsible. Dell is a member of the Electronic Industry Citizenship Coalition (EICC), and we adhere to the Electronic Industry Code of Conduct. We are committed to working with socially responsible entities that comply with all applicable

laws and regulations where they conduct their business, embrace high standards of ethical behavior, and treat their employees fairly, with dignity and respect. Both Dell and the EICC audit for adherence to applicable laws regulating wages, hours and working conditions. Dell requires its suppliers to implement the EICC code of conduct. Suppliers must demonstrate a commitment to the health and safety of their employees and not use forced or indentured labor, or use raw materials or finished goods produced by forced or indentured labor.

Dell is also committed to protecting the privacy of our customers. Our privacy statement makes clear that Dell will only collect, store and use their personal information for limited business purposes and to support and enhance our relationships with them. We do not sell our customers' personal information. We expect our employees to appropriately safeguard our customers' information and comply with Dell's privacy policies and applicable laws on customer privacy.

Dell's Approach to Government Mandates and the Global Network Initiative

As you recognize in your letter, access to technology and the Internet is critical in promoting human rights and freedom of expression around the world. Dell is proud of our role in placing this powerful tool in the hands of our global customers. We recognize, however, that issues may arise with respect to government mandates that may impact customers in a particular country.

When facing specific government mandates where that country's customers' freedom of expression or privacy may be impacted, Dell has sought guidance from our own Code of Conduct as well as applicable best practices. In this regard, Dell is familiar with the GNI principles and guidance, which generally mirror our approach. For example, in assessing any situation, Dell seeks to avoid or minimize the impact of government mandates or restrictions on freedom of expression and privacy.

We recognize that issues involving governmental policies are bigger than any one company's ability to deal with effectively, and so we attempt to modify such mandates by working with other companies that may be similarly affected using our trade associations, and engaging with the local governments directly, through our associations.

We strive to provide customer choice when at all possible, consistent with local law. If not possible, then we work to narrowly tailor any mandated approach to protect customer freedom of expression and privacy as much as possible. We also seek to give clear, prominent, and timely notice to customers when access to content has been limited due to government restrictions.

Dell recognizes the value of industry best practices in this area, and we are open to discussing the value of GNI membership as well as other options specifically tailored to the IT hardware sector. We know that one of our leading technology trade associations, the Information Technology Industry Council, is developing a list of principles designed to meet the specific needs and issues faced by hardware industry.

We appreciate your work to protect human rights around the world. Dell remains committed to protecting human rights, whether with respect to our own employees, our suppliers and their workers, or customers.

Sincerely,

A handwritten signature in black ink, appearing to read "Gilbert F. Casellas". The signature is fluid and cursive, with the first name being more prominent.

Gilbert F. Casellas
Vice President
Corporate Responsibility
Dell Inc.



eBay Inc.
2005 Hamilton Avenue
San Jose, California 95125

September 1, 2009

www.ebay.com

The Honorable Richard Durbin
Chairman
Subcommittee on Human Rights and the Law
United States Senate
Washington, DC 20510

The Honorable Tom Coburn
Ranking Member
Subcommittee on Human Rights and the Law
United States Senate
Washington, DC 20515

Dear Senators Durbin and Coburn:

Thank you for your letter dated August 6th regarding the "Global Network Initiative" and your ongoing efforts to protect human rights through the Internet, communications and technology sectors. As a global business, eBay Inc. takes the issues raised in your letter seriously and we appreciate your leadership on this issue.

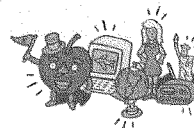
As you may be aware, for the past four years eBay Inc. has been made up of three primary business units: marketplaces, payments and communications. Our communications business, Skype, has been engaged in ongoing conversations with the founders of the Global Network Initiative "GNI" for the past year and accordingly its President, Josh Silverman, has responded fully to your inquiry.

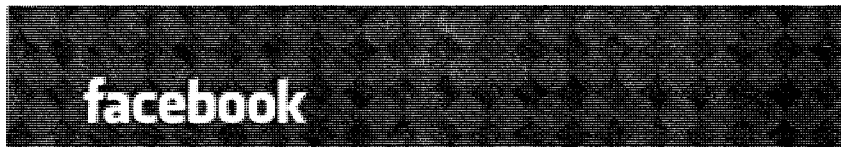
Nonetheless, addressing the fundamental moral, legal and regulatory matters you have identified are of critical concern to businesses such as eBay that operate on a global basis. It is worth emphasizing that eBay's payments and marketplaces businesses raise few if any of the issues currently being addressed by the GNI or the related legislative deliberations. However, with the proposed sale of a majority ownership in Skype, and the expressed interest of leading policymakers such as you in the further development of the GNI effort, eBay representatives will be participating in upcoming meetings related to the appropriate development and expansion of the regime.

Should you have any additional questions or concerns as this multiparty initiative moves forward, please do not hesitate to contact me.

Regards,

John Donahoe
President and CEO





August 27, 2009

The Honorable Richard J. Durbin
 Chairman, Subcommittee on Human Rights and the Law
 U.S. Senate Committee on the Judiciary
 224 Dirksen Senate Office Building
 Washington, DC 20510

The Honorable Tom Coburn
 Ranking Member, Subcommittee on Human Rights and the Law
 224 Dirksen Senate Office Building
 Washington, DC 20510

Dear Chairman Durbin and Ranking Member Coburn,

We write in response to your request for information regarding Facebook's commitment to respecting and advancing human rights and to thank you for inviting us to join the Global Network Initiative. At Facebook, we share the goals of GNI and work hard every day to provide a tool that enables hundreds of millions of people around the world to support these same goals through personal connection, communication and sharing. In fact, for us, these values are foundational since our corporate mission is "to give people the power to share and make the world more open and connected." We are proud of the Facebook's users playing in promoting human rights and would offer two recent examples that illustrate the effectiveness of our service to promote these goals:

- In January 2008, Oscar Morales, an engineer from Bogota created a Group on Facebook called "Un Millon de Voces Contra las FARC" ("One Million Voices against the 40-year-old terrorist organization, Fuerzas Armadas Revolucionarias de Colombia"). Just over a month later, the world watched as simultaneous marches against FARC happened all over the globe. Spain's EFE news service estimated that more than 10 million took to the streets as a result of the Facebook group, which was used to coordinate the demonstration.
- As recently as June of this year, Facebook's users played a role in the Iranian elections and the protests that followed. We encouraged Iranians on Facebook to vote, by providing a vote-counter that people could click on to say they voted, and they could also demonstrate to their friends their participation if they chose to. When citizens and

observers became suspicious of the outcome of the election, they used Facebook as a mechanism to share information and organize. This was made easier by our timely introduction of a new interface for Facebook that was translated into Farsi. Once the government began to crack down on protest, troubling accounts, videos and photos of the violence got out of Iran and were shared globally by some users through Facebook and other services.

You have our commitment to assist our users as they engage in activism similar to that mentioned above. In addition, we are and will continue to look for specific ways that we enhance Facebook to help others protect and promote human rights. We also commit to continuing the dialogue with you and other experts to help us in these efforts.

Finally, Facebook submits the following answers to specific questions posed by the Subcommittee regarding Facebook's approach to advancing human rights and the Global Network Initiative ("GNI"):

1. What are your company's views of GNI?

Facebook admires the GNI and appreciates that the GNI's principles and the commitments of its signatories mirror the commitments that Facebook has embodied in its behavior and governing documents, including our Statement of Rights and Responsibilities, Privacy Policy, and Facebook Principles. The GNI has already and will continue to encourage technology corporations to respect and promote users' human rights.

We also recognize that the GNI exposes important tensions between how to make real both free speech and privacy in countries with different traditions and values. Whereas the dominant belief in some countries is that restrictions on the free flow of information promote greater harmony and political stability, in the U.S. most believe that greater openness and transparency will promote social harmony and political stability. These conflicting approaches present challenges for companies, particularly ones such as Facebook that are small and growing, to navigate new markets around the world without strong support from national governments and multilateral institutions

2. Will your company consider joining the GNI? If yes, please describe the process you will follow to consider joining the GNI. If no, why not?

Facebook is committed to advancing the human rights of freedom of expression and personal privacy. However, as a young start-up, our resources and influence are limited. We have dramatically fewer employees than most of the GNI members, in some cases totaling one percent the size of GNI participants. We are dedicated to building and improving a free service that

1601 S. California Avenue, Palo Alto, California 94304
650.543.4800 - tel 650.543.4801 - fax

fosters sharing and connecting and that, thereby, aids our users in promoting and protecting human rights. While we do not have the resources to devote to GNI membership, we certainly do remain actively engaged with GNI members on these issues of importance. Moreover, we commit to devoting resources to continuing to foster activism, organizing and communicating around human rights issues among our growing global community of users. In addition, we hope to continue the dialogue with you and other experts to help enhance the service for the promotion of human rights and remain in contact for such time when we do have the resources to join and support GNI.

In the meantime, we would respectfully submit for your consideration the idea that our efforts and those of GNI could be magnified significantly by bringing the U.S. government to bear in multilateral trade negotiations that make clear it is U.S. government policy that maximizing free speech through modern communications systems is an important U.S. value. Could we collaborate in promoting this idea to your colleagues? Governments, not companies, are best suited to advancing human rights and alleviating pressures on companies.

3. Does your company currently follow any of the GNI principles?

Facebook works diligently to advance both individuals' freedom of expression and right to personal privacy. Despite our resource constraints, Facebook is advancing individuals' free speech around the globe by facilitating sharing and connecting of users. Facebook is a free service, and we provide the ability for anyone anywhere to share any piece of information – musings, comments, articles, photos, and videos – with anyone, anywhere. The freedom of expression of our 250 million users worldwide is limited only by (i) a users' access to internet service; (ii) laws limiting sharing of copyrighted or trademarked materials; (iii) our user agreements that include a commitment to abide by Facebook's community standards outlined in our Statement of Rights and Responsibility; and (iv) local laws in jurisdictions around the world.

We believe we help our users overcome unnecessary barriers to free speech. In addition to giving users the ability to quickly and easily publish their views to their friends and the world, Facebook also facilitates two-way conversations between citizens and their leaders. Government officials and agencies across the globe are now utilizing Facebook to engage in direct, ongoing conversations with the public. No longer do you need status or wealth to distribute your ideas widely, or to have your opinions be heard by your government. For example, President Obama has held multiple Facebook-hosted events where he received and responded to questions in real time that were posed by the public, and one need only follow the news to hear about countless other examples where Facebook has been used to facilitate dialogue.

Facebook's advancement of free speech in countries and regions where repression is used to silence critics is equally well documented. As mentioned earlier, Facebook served as a venue

1601 S. California Avenue, Palo Alto, California 94304
650.543.4800 - tel 650.543.4801 - fax

for Iranians to rally around their election candidates, debate the results of their election and protest against actions taken subsequently to squelch debate. As a result, Facebook's users made Facebook a vital conduit during this important world event.

Similarly, Facebook's approach to privacy by providing users maximal control over data empowers users to share more. Thus, our privacy policy likely supports and encourages free speech in a symbiotic fashion. All of our privacy statements are written in plain language. Our users provide us with personal information and entrust us to share it only at their direction and only with the people they choose. We are constantly working to improve the privacy controls we provide, and our recent innovations include the announced roll-out in the near future of the Publisher Privacy Control, which will allow people to easily choose an audience for each piece of content or information they choose to share at the exact time that they share it. Facebook is not aware of any other major technology that provides users with this type of granular control over their speech and sharing of data. This concept of the power to publish coupled with user control over the audience, we believe encourages users to exercise their speech rights more routinely and without concerns about censorship.

4. Please describe your company's policies and practices for advancing and protecting human rights and minimizing the risk that your products and/or services will facilitate human rights abuses.

While as a relatively resource-constrained, small company Facebook cannot currently commit to the extensive implementation guidelines that the GNI signatories agree to, Facebook carefully evaluates new markets with an eye towards human rights. Each time Facebook considers engaging in commerce in a new country, Facebook evaluates whether the laws, policies and mores of that country share Facebook's commitment to openness, sharing and transparency and, if not, what accommodations may be necessary to advance our goals of sharing and user control. If we are not prepared to make the accommodations required, we will not do business in that market.

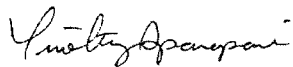
In addition to the efforts described above, Facebook goes to great lengths to maintain the confidentiality of users' account information and to protect against spying or monitoring by repressive foreign regimes. Facebook's governing documents, which are available to all users, clearly state that Facebook only complies with valid legal requests for data by law enforcement or government agencies. Consequently, Facebook closely scrutinizes all requests for data, and we do not reveal any data unless we have a good faith belief that a request meets applicable legal standards.

1601 S. California Avenue, Palo Alto, California 94304
650.543.4800 - tel 650.543.4801 - fax

Additionally, Facebook safeguards users' privacy and advances free speech by resisting attempts by governments to require that companies engage in so-called "data retention." Some officials, including some Members of the U.S. Congress, have sought to require that all Internet companies retain all of their users' data for a set minimum period of time. Some of these proposed data retention mandates would include a requirement that companies retain metadata, i.e., the transactional information that could show with whom a customer is interacting, where parties to a conversation are located, when and for how long they were using a specific technology to communicate, and what sites they visited on the Internet. Currently, Facebook purges its servers of much user-generated data, including metadata, after a short period of time to conserve server space and protect users' privacy. Facebook also allows users to delete their accounts to protect their privacy. Facebook is resisting data retention mandates because the lack of a retention mandate allows us to limit the amount of data we store, and the length of time that we store it. The result is that we cannot comply with certain data requests as we promptly and routinely overwrite data on our servers that is not necessary to be retained for the operation of the site, is metadata, or is the data of an account that has been deleted.

Facebook thanks the Subcommittee for its solicitation of Facebook's opinions with respect to these important topics and again advocates for articulation of U.S. trade policy that establishes that penalizing U.S. companies for facilitating free speech and privacy is a non-tariff trade barrier. Facebook also encourages U.S. government engagement with other nations to harmonize human rights standards to benefit individuals everywhere and facilitate commerce respectful of human rights.

Sincerely,



Timothy Sparapani
Director, Public Policy
Facebook, Inc.

1601 S. California Avenue, Palo Alto, California 94304
650.543.4800 tel 650.543.4801 - fax



By Facsimile and Email

August 27, 2009

U.S. Senator Richard J. Durbin
 U.S. Senator Tom Coburn
 United States Senate
 Washington, DC 20510
 Facsimile: c/o Heloisa Helena Griggs at (202) 228-0781
 Email: c/o Lauren Myerscough-Mueller at Lauren_Myerscough-Mueller@Judiciary-dem.senate.gov and Heloisa Helena Griggs at Heloisa_griggs@Judiciary-dem.senate.gov

Dear Senators Durbin and Coburn:

Thank you for your letter dated August 6, 2009. We appreciate the information you provided on the Global Network Initiative, or GNI, and we are happy to discuss this further with you and your staff.

To initiate those discussions, Renee Roe and I called Heloisa Helena Griggs, Counsel to U.S. Senator Richard J. Durbin, and had a good conversation with her yesterday regarding the GNI.

Fortinet is reviewing the GNI program, and, per Ms. Griggs's suggestion, we intend to reach out directly to the GNI for additional information to better understand the program and the degree to which Fortinet joining the program would have a positive impact.

Please feel free to contact me directly on this matter if you would like to discuss further.

Sincerely,

FORTINET, INC.

John Whittle
 Vice President, General Counsel

cc: Ken Xie, CEO, Fortinet
 Renee Roe, Global Trade Compliance Officer, Fortinet

1090 Kifer Road, Sunnyvale, CA 94086
 Tel: 408.235.7700 Fax: 408.235.7737

Bruce Ives
Vice President and
Deputy General Counsel
Global Alliances & Government Affairs
650.857.8780 Tel
650.852.8617 Fax
bruce.ives@hp.com



Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1112
www.hp.com

August 27, 2009

The Honorable Richard J. Durbin
United States Senate
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom Coburn
United States Senate
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Senators Durbin and Coburn:

Thank you for your letter of August 6, 2009, regarding Hewlett-Packard's approach to human rights issues and the Global Network Initiative (GNI). As always, we welcome open and constructive dialogue about our corporate social responsibilities and commitment to promoting human rights.

I agree with you on the value of initiatives like GNI to promote ethical decision-making by businesses and to ensure businesses are not complicit in human rights violations. At HP, we take these issues very seriously. We operate around the world under one, high-level code of conduct and set of policies designed to ensure that we behave ethically as a company and respect human rights (including in the areas of privacy and free expression). We pursue these objectives through rigorous internal corporate policies and procedures as well as through external engagement, including by engaging with stakeholders, other businesses, and outside institutions in collaborative processes to advance shared values. Moreover, HP subjects itself to internal and third-party assessments and evaluations of our performance. We repeatedly have received favorable recognition for our efforts.

First, HP has integrated human rights principles into business decision-making. For example, we have a strong set of policies that all employees must follow. Under the Global Citizenship Policy, all employees must uphold the human rights articulated in the Universal Declaration of Human Rights, which includes the freedom of expression and the right to hold opinions without interference. HP's Standards of Business Conduct require all employees to support and respect the protection of human rights. In the privacy sphere, HP's Global Master Privacy Policy protects personal information against unauthorized use or disclosure and prohibits the transfer of such personal information to third parties, unless those third parties promise to give the data the equivalent level of

Bruce Ives
Vice President and
Deputy General Counsel
Global Alliances & Government Affairs



Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1112
www.hp.com

August 27, 2009
Page 2

protection that HP provides. Finally, HP's Human Rights & Labor Policy embeds international human rights standards in HP's global personnel policies and guidelines.

Our efforts even extend beyond areas where we have operational control. For example, HP's Supplier Code of Conduct promotes responsible practices in labor, human rights, ethics, the environment, and worker health and safety at our suppliers. Our supply chain program promotes respect for the human rights and labor conditions of more than 340,000 workers worldwide. In 2008, HP audited 129 supplier sites for compliance with this code of conduct, bringing our total since 2005 to 480. Ninety-nine of our 2008 audits were follow-up audits, which demonstrated substantial progress in reducing instances of non-conformance found during initial reviews.

To maximize enforcement of HP policies, we provide multiple anonymous channels for employees to report any noncompliance or ethical concerns. Our Chief Ethics and Compliance Officer oversees these mechanisms, processes all reports, and reports independently to the Audit Committee of the Board of Directors.

HP's staunch commitment to human rights is also reflected in our corporate governance structure. Our Global Citizenship Council, which comprises senior executives, meets regularly to coordinate HP's global citizenship strategy across the company. Our global citizenship framework consists of five core areas: ethics and compliance, environmental sustainability, human rights and labor practices, privacy, and social investment. To that end, the Council includes the key corporate leaders who have the functional responsibility to integrate these considerations into our business. Members include the Global Citizenship Vice President, Chief Privacy Officer, Corporate Strategy Director, Supply Chain Director, Human Resources Director, Environmental Sustainability Director, Social Investment Director, Government Affairs Vice President, and Chief Ethics and Compliance Officer. The Council advises HP's Executive Council—a body that includes HP's Chief Executive Officer and the heads of each HP business unit—which retains overall responsibility for global citizenship as part of our business strategy. The Executive Council, in turn, reports directly to the Board of Directors.

In short, responsible global citizenship is a corporate objective for HP, and this mission is prioritized at the highest levels of the organization.

Second, beyond internal initiatives, HP proactively collaborates with multiple stakeholders, other businesses, and institutions to advance our commitment to human rights and more broadly global citizenship. Our external engagement comprises initiatives to advance the range of global citizenship issues as well as more targeted initiatives specific to our business.

In terms of wider-ranging initiatives, we have been a member since 2002 of the UN Global Compact, which sets forth ten universally accepted principles to which

Bruce Ives
Vice President and
Deputy General Counsel
Global Alliances & Government Affairs



Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1112
www.hp.com

August 27, 2009
Page 3

participating companies must try to align their business operations and strategies. The UN Global Compact is based on the principles of the Universal Declaration of Human Rights, which is the foundation of the international human rights system and protects freedom of expression and privacy. As a member of the UN Global Compact, HP's commitment extends to Principles 1 and 2, which state: "Businesses should support and respect the protection of internationally proclaimed human rights; and make sure that they are not complicit in human rights abuses."

HP has also played a key role in the Business Leaders Initiative on Human Rights, a group of 16 global companies (including Coca Cola, General Electric, and Gap) that developed a step-by-step guide for businesses to integrate Universal Declaration of Human Rights principles (again, which include the freedom of expression and privacy) into their management decision processes. This guide was developed in cooperation with Realizing Rights: The Ethical Globalization Initiative and the UN Office of the High Commissioner for Human Rights and includes a Business and Human Rights Matrix, which helps companies conduct self-assessments and identify any gaps between their policies and international human rights standards. Former UN High Commissioner on Human Rights Mary Robinson chaired this effort.

HP has also been a leader in addressing the primary human rights challenges that are specific to our business. In 2003, HP helped found the Electronic Industry Citizenship Coalition. In collaboration with Dell, IBM, and other electronics manufacturers, this organization developed the Electronic Industry Code of Conduct, which outlines standards to ensure that working conditions in the electronics industry supply chain are safe, that workers are treated with respect and dignity, and that manufacturing processes are environmentally responsible. Because this initiative addressed an issue that is core to HP's particular business, we were able to add significant value and are driving meaningful change in this area.

Third, we are committed to transparency to allow inside and outside actors to credibly assess and evaluate HP's human rights performance. Pursuant to the UN Global Compact's reporting requirements, HP publishes an annual public Global Citizenship Report, which the UN Global Compact Office has officially recognized for its high quality and comprehensiveness. The report provides detailed reporting on HP's ethics and compliance program, our ongoing privacy initiatives, and our human rights practices.

HP has invited outside stakeholders to help assess our performance and provide guidance going forward. For instance, in 2007, we established the Stakeholder Advisory Council (SAC), which comprised five prominent NGO representatives as well as senior HP executives. The SAC met regularly, and the NGO members helped us identify and prepare for potential business risks and provided advice on our leadership strategy for our global citizenship initiatives. In late 2008, HP expanded and renamed

Bruce Ives
Vice President and
Deputy General Counsel
Global Alliances & Government Affairs



Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1112
www.hp.com

August 27, 2009
Page 4

the SAC as the Trusted Advisory Network (TAN). And, as noted, HP provides internal mechanisms to ensure accountability such as channels for whistleblowers to report any noncompliance or ethical concerns.

HP consistently has earned good marks from NGOs and others for our actions and policies. Students and Scholars Against Corporate Misbehavior (SACOM), a Hong Kong-based NGO that monitors corporate behavior and advocates for workers' rights, wrote in a 2008 report that "Hewlett Packard is setting the pace for social responsibility in China." In February 2009, Corporate Responsibility Officer (CRO) ranked HP number 5 on CRO's 100 Best Corporate Citizens for 2009. On the rare occasion when the human rights community has criticized HP, we have been very responsive. For example, CSR Asia—a consultancy focused on sustainable business practices in Asia—recently commended HP for our responsiveness to a report that was critical of our supplier factories' working conditions.

As you can see from these initiatives, HP has pursued our commitment to global citizenship, including human rights, ambitiously and comprehensively. We have devoted significant resources to these efforts and pursued them with a long-term approach that involves integrating human rights considerations into our business practices. These efforts are multi-year commitments, and HP continues to leverage its past efforts and build upon the foundation that it has collaboratively laid with multiple stakeholders. For example, HP has engaged in the Business Leaders Initiative on Human Rights for the past five years, and we recently renewed our commitment for another three years to the successor organization (Global Business Initiative on Human Rights). Going forward, that organization will be dedicated to promoting assessment tools and institutionalizing human rights principles (including those of freedom of expression and privacy) in corporate governance. We similarly have made a long-term commitment to the Electronic Industry Citizenship Coalition and continue to help drive our industry's engagement on supplier issues. It is in initiatives like these and through our leading efforts with respect to our Supplier Code of Conduct where companies in our sector can make maximum contribution to promoting human rights.

I hope the above makes clear that HP fully supports GNI's principles as we have already embedded the core ones—such as responsible company decision-making, multi-stakeholder collaboration, and accountability/transparency—into our business operations. In the past, we have considered, but not pursued, membership in GNI because the primary challenges that we face are generally not the same as those faced by online service providers, the founding focus of GNI. For instance, supply chain management, working conditions, privacy, and environmental sustainability are central issues for a company like HP, and we have grappled with them seriously through internal policies and collaborative engagement. We believe that the diversity of approaches that companies, NGOs, and other stakeholders pursue to ensure

Bruce Ives
Vice President and
Deputy General Counsel
Global Alliances & Government Affairs



Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1112
www.hp.com

August 27, 2009
Page 5

responsible corporate conduct is healthy, and ultimately serves the common goal of promoting respect for human rights.

When we consider participating in any new initiative, such as GNI, we consider a variety of factors, including: whether joining the initiative would dilute our ongoing human rights efforts or detract from our sustained focus on areas where we are already committed; whether it is an initiative where we can add maximum value, given the nature of our business and the challenges germane to it; and whether the initiative would be duplicative of existing efforts. Based on our engagement to date, we do not see that HP participation in GNI would, on balance, advance our ongoing efforts to ensure responsible corporate conduct. We believe our current work in the area of global citizenship is robust, adaptable to emerging issues, and tailored to maximize our impact given the sectors in which we operate. Nonetheless, we are open to learning more about GNI.

I look forward to our continued work with you on this and many other important issues.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Bruce Ives', with a stylized flourish at the end.

Bruce Ives

1333 New Hampshire Avenue, NW
Washington, DC 20036
www.lenovo.com

August 14, 2009

Senator Richard Durbin
309 Hart Senate Office Building
Washington, D.C. 20510

Senator Tom Coburn
172 Russell Senate Office Building
Washington, D.C. 20510

Re: The Global Network Initiative

Dear Senators Durbin and Coburn:

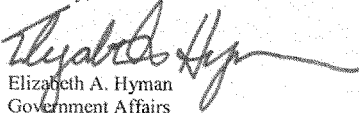
Thank you for your letter of August 6th regarding the Global Network Initiative (GNI). First, we wish to note for clarification that it was Rachel Adams and Elizabeth Hyman (not Mr. Yang Yuanqing CEO of Lenovo) who were pleased to attend the meeting with your staff on July 30, 2009.

Lenovo appreciates your inquiry with respect to the GNI and shares your deep concern for global human rights. Indeed, Lenovo is committed to being a responsible and active corporate citizen, consistently working to improve our business while contributing to the development of communities in which we do business.

To that end, we are an active member in the Electronics Industry Citizenship Coalition and an adherent to the EICC code of conduct for the global electronics supply chain. The code drives improvement in global working and environmental conditions. Lenovo is a signatory to the UN Global Compact, a strategic policy initiative for businesses committed to aligning their operations and strategies with ten universally accepted principles in the areas of human rights, labor, environment and anti-corruption.

We are evaluating your letter and the mission and objectives of GNI and intend to provide a response. Lenovo is also committed to work with the relevant trade association(s) in evaluating the GNI and its mission. As your staff noted, however, the GNI is a significant and complex initiative. Given that complexity, and in light of summer schedules and the unavailability of key Lenovo personnel at this time, we are not in a position to meet your short turn-around time of August 27, 2009. We will, however, respond as soon as practicable and after we have carefully evaluated the matter.

Sincerely,


Elizabeth A. Hyman
Government Affairs

New World. New Thinking.

lenovo

Gregory Q. Brown

President & Chief Executive Officer

August 21, 2009

The Honorable Richard J. Durbin
The Honorable Tom Coburn
United States Senate
Washington, DC 20510

Dear Senators Durbin and Coburn:

Thank you for your letter regarding human rights and the Global Network Initiative (GNI).

Motorola is a strong proponent of protecting human rights, as expressed in our Human Rights policy (www.motorola.com/humanrightspolicy), Code of Business Conduct (www.motorola.com/code), Supplier Code of Conduct (www.motorola.com/suppliers/code), and Environment, Health and Safety policy (www.motorola.com/ehspolicy). Motorola's human rights policy is based on our long-standing key beliefs of uncompromising integrity and constant respect for people, and is consistent with the core tenets of the International Labour Organization's fundamental conventions and the United Nations Universal Declaration of Human Rights.

We agree that Information and Communications Technology (ICT) companies should respect and protect the freedom of expression and privacy rights of their employees and users. The power of ICT should be used globally to support economic opportunity, advance knowledge and improve the quality of life.

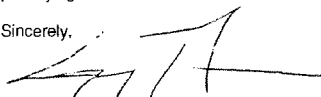
For example, Motorola participates in Phones for Health, a public-private partnership that uses the increasing mobile phone coverage in the developing world to strengthen health systems. A mobile-phone-based application allows health workers in the field to file patient reports and check medicine supplies, speeding responses to disease outbreaks and medicine shortages. The mobile phone transfers the data to a central database, where the data is mapped, analyzed and immediately available to health authorities, allowing rapid intervention for those at risk. The program currently is available in Kenya, Rwanda and Tanzania with plans to expand to several more countries.

Motorola works to enable freedom of expression and protect people's privacy, which we recognize are human rights that facilitate the meaningful realization of other human rights. The mobile phone is all about freedom of expression and allows people to connect and communicate more easily and rapidly than ever before. We believe that people have the right to control their personal information, determining how it is collected and used. We are committed to protecting the privacy of those who submit personal information to Motorola. We train our employees on our privacy policies and practices, and we provide additional support for people whose jobs involve handling personal information. We work closely with third parties handling personal information on our behalf to ensure that the highest privacy standards are maintained. Employees who violate our information protection policies are subject to disciplinary action, including dismissal. Agents and subcontractors face contractual penalties or termination.

We build certain technologies into our products to allow our customers to better protect their personally identifiable and confidential information. Our products are designed to protect the users' privacy and security. We include technology to guard against external interference and provide voice data encryption on mobile phone networks. Our mobile phone user manuals provide information about privacy and security risks, highlighting privacy and security protection functions.

Thank you for reaching out to Motorola on this important issue. We will continue our efforts to protect human rights and encourage companies to follow policies and guidelines that respect and protect freedom of expression and privacy rights.

Sincerely,



Greg Brown

Motorola, Inc., Corporate Offices
1303 E. Algonquin Rd., Schaumburg, IL 60196 U.S.A. Tel: +1 847 576 1993 Fax: +1 847 576 0079



News Corporation

1211 AVENUE OF THE AMERICAS • NEW YORK, NY 10036 • 212-852-7100 • FAX: 212-852-7094

RUPERT MURDOCH, A.C.
CHAIRMAN AND CHIEF EXECUTIVE OFFICER

August 24, 2009

The Honorable Richard J. Durbin
Chairman
Human Rights and the Law Subcommittee
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tom Coburn
Ranking Member
Human Rights and the Law Subcommittee
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Senators Durbin and Coburn,

Thank you for your letter dated August 6, 2009 regarding the "Global Network Initiative" (GNI). The free flow of information and freedom of expression are fundamental to News Corporation's business as a global media and entertainment company. We also recognize the importance of respecting the privacy of our customers and users. We therefore welcome your attention to these critical issues.

I am aware of the GNI and News Corporation is supportive of its work. News Corporation's MySpace, Inc. has been thoroughly reviewing the Principles, Implementation Guidelines and Accountability Framework of the Initiative and we continue to monitor its progress.

I will endeavor to answer the questions you pose in your letter by describing MySpace Inc.'s Chinese business arrangements, its general practices regarding content and law enforcement cooperation and the international restructuring it is currently undergoing.

MySpace, Inc. licensed its brand and technology to a social networking site in China formerly known as MySpace.cn (for ease of reference I will continue to refer to it as such in this letter, though the name of the site has been changed). MySpace.cn, a locally owned, operated and managed company, is responsible for implementing measures to ensure compliance with Chinese law. MySpace.cn discloses to its users prior to their registration that it is a Chinese site subject to Chinese law.

MySpace, Inc. also operates MySpace.com, the English language U.S.-based site that remains available to all Internet users around the world. MySpace.com hosts its user data and content in California and is therefore governed by U.S. law. It does not filter or block content based on foreign laws related to content restrictions, but rather has established and enforces content rules in the Terms of Use that are posted on every page of the site. MySpace.com will respond to takedown requests from third-parties if it determines that the content in question violates MySpace.com's Terms of Use. MySpace.com will also respond to law enforcement requests for data in a manner consistent with U.S. law.

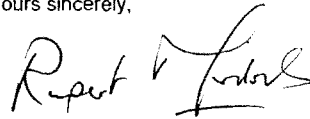
Indeed, foreign law enforcement requests are subject to the Mutual Legal Assistance Treaty when content, rather than traffic and registration data, is being sought.

MySpace, Inc. recently announced that it will undergo a restructuring that will narrow its operations to a limited group of countries, and is currently in the process of implementing various restructuring decisions.

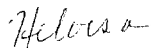
In light of MySpace.com's compliance with U.S. law and MySpace, Inc.'s evolving international arrangements and operations, we have not joined GNI. As noted above, however, we are supportive of its work and will continue to monitor its activities.

Thank you for your leadership on this important issue and we look forward to working with you to bolster the commitment to the freedom of speech and the privacy of users both in the U.S. and abroad.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Rupert Murdoch", with a stylized flourish at the end.

Rupert Murdoch
Chairman


NOKIA

 OLLI-PEKKA KALLASVUO
 President and CEO

August 27, 2009

1 (4)

The Honorable Richard J. Durbin
 Chairman, Subcommittee on Human Rights and the Law
 United States Senate
 Washington, D.C. 20510

The Honorable Tom Coburn
 Ranking Member, Subcommittee on Human Rights and the Law
 United States Senate
 Washington, D.C. 20510

Dear Chairman Durbin and Ranking Member Coburn,

Thank you for your letter of August 6, 2009 regarding Nokia's approach to human rights issues and our views on the Global Network Initiative (GNI). I appreciate this opportunity to explain Nokia's deep commitment to human rights and the improvement of the lives of billions of people around the world we enable with our products and services.

As you note in your letter, information and communications technology (ICT) has enhanced human rights and the freedom to communicate for people all around the globe. Nokia has long recognized the power of communication to improve the lives of human beings and believes it is a basic human right that we are making real for everyone. Indeed, "Connecting People" is our corporate motto and our role in facilitating communication for billions of people is a source of immense pride for us. The rapid spread of information, opinions and ideas is greatly enhanced through the use of mobile technology and Nokia believes our users should be able to create and communicate ideas and information without regard to where they live or what type of communications technology they use. Today over four billion people in the world use mobile phones, making this technology the most powerful communications tool in the history of mankind. The convenience and freedom mobile technology brings has been shown on numerous occasions to be a powerful enabler of the sharing of information and ideas and the development of democracy.

Nokia also believes there is a strong link between mobile technology and economic and social development and that our products and technologies contribute positively to human rights, the environment and in the development of many societal areas. Beyond just providing basic voice communications to people, we believe that individuals, communities and nations worldwide can and should have affordable access to all the social and economic benefits that mobile technology can offer. Nokia is deeply involved in the development of agricultural, financial, health care and educational mobility solutions aimed primarily at users in the developing world and emerging markets. We believe these solutions will improve the overall well-being of people, resulting in stronger, more stable and more democratic societies.

NOKIA CORPORATION
 P.O. Box 226, FI-00045 NOKIA GROUP, Finland
 (Street address: Keilalaudentie 2 A, 00130 Espoo)

Tel: +358 7 130 34474
 Fax: +358 7 180 38684

Business Identity Code 0112048-9
 Helsinki

NOKIA

2

Nokia sells over 1 million mobile devices per day around the world and while we are expanding our business to include services and solutions such as reselling music for mobile devices and the aforementioned solutions for agriculture, education and health, we are primarily a manufacturer mobile telephones and other mobile communications devices. Since 1997 Nokia has had a Code of Conduct to ensure we engage in ethical, responsible and sustainable business practices and to guide us in difficult situations on how to live up to the highest ethical standards we have set for ourselves (for your convenience, we have attached a copy of the latest version of the Nokia Code of Conduct). While the Code has undergone several revisions over the years to ensure that it reflects the external environment and current business issues, its fundamental principles are the same and are based in Nokia's values. Specifically, the Code requires that Nokia and its employees will respect human dignity and promote human rights, will be environmentally aware in all that we do, will have zero tolerance for corruption and will foster diversity and equal opportunity. In addition, as part of our strict supply chain requirements, Nokia requires its business partners, subcontractors, or suppliers to comply with all applicable laws and regulations. We strongly encourage our partners, subcontractors, and suppliers to strive further than just legal compliance in areas such as corporate governance, human rights and the environment. We also incorporate ethical, social and environmental criteria in our procurement agreements, and commit to monitoring the performance of our partners and take immediate and thorough remedial steps in cases where the ethical performance of our business partners comes into question.

As described in our Code of Conduct, Nokia will respect and promote human rights. Nokia recognizes, with the international community, that human rights should be considered fundamental and universal, based on accepted international laws and practices, such as those of the United Nations' Universal Declaration of Human Rights, the International Labour Organization and the United Nations Global Compact (UNGC) principles. Among those rights that Nokia views as fundamental and universal are: Freedom from discrimination on any grounds; freedom from arbitrary detention, execution or torture; freedom of peaceful assembly and association; freedom of thought, conscience and religion; and freedom of opinion and expression.

Nokia respects and protects the freedom of expression of users by seeking to avoid or minimize the impact of government restrictions on freedom of expression, including restrictions on the information available to users and the opportunities for users to create and communicate ideas and information, regardless of frontiers or media of communication.

Internally, issues concerning ethics, privacy, human rights and corporate responsibility are handled by Mr. Esko Aho, Nokia's Executive Vice President of Corporate Relations & Responsibility. Mr. Aho is a member of the Nokia Group Executive Board and reports directly to me. Prior to joining Nokia, Mr. Aho was a long-serving member of the Finnish Parliament and the Prime Minister of Finland from 1991 to 1995. Mr. Aho has a deep understanding of human rights issues and the roles that governments, companies and civil society must play to ensure that human rights are preserved and protected.

Nokia has a defined internal process for addressing instances where law enforcement officials or other government entities that claim legal authority request Nokia to either disclose information on Nokia employees or customers or restrict access to data that may involve issues of freedom of expression or privacy. Any employee who receives such a request must follow a defined, internal issues response management process and an internal task force is created involving local legal as well as global privacy counsel to evaluate and respond to such requests in the most appropriate and timely way.

NOKIA

3

The requests are thoroughly vetted internally pursuant to guidelines that incorporate international legal standards that are similar to those incorporated by the GNI. In particular, we first verify the legal validity of the request and the right of the entity to make the request, under both local law and international laws and norms. In many cases, we direct the requesting entity to contact the relevant authorities in the country where the data owner is based, which for Nokia is generally Finland. Finnish authorities will then verify the legality of the request before contacting us. In those cases where the request has been determined to be legal and valid, we define the requests narrowly in order to minimize the amount of data we provide and the potentially adverse impacts on privacy and freedom of expression. As with the GNI implementation guidelines, we require requests to be in writing and we respond to requests only in writing, encrypting the content of the response and sending a password separately. Finally, we provide clear notice to users when data has been provided or access to data limited pursuant to a request, and describe the reasons for such actions.

As described above, Nokia is strongly committed to protecting and advancing human rights such as freedom of expression and privacy in our business. Indeed, these principles are ingrained in our corporate values and we have long incorporated them in our Code of Conduct and our business practices. In fact, Nokia has already committed to follow these principles through our active involvement in several well-recognized industry and government organizations such as the Global e-Sustainability Initiative (GeSI), the European Alliance for CSR, and the UNGC.

Nokia has been a signatory of the UNGC since nearly its inception and we believe that it is remarkable that over 5200 participants from 130 countries representing all industrial sectors (including Alcatel-Lucent, Accenture, Ericsson, Ford, Cisco, Hewlett-Packard, Intel, Hitachi, Microsoft, Merck, General Electric, DuPont, Coca Cola, PepsiCo) have expressed their commitment to following its human rights principles and report their progress annually. The breadth of the UNGC's membership by companies in all sectors operating throughout the world, rather than focusing on just one sector, makes it more likely to effect change in behavior and attitudes in all levels of the economy. The UNGC offers guidelines and publications that help institutions define human rights, outline international obligations and ways to address human rights concerns with local custom and laws. There are also regional venues for addressing concerns if needed. This material is publicly available, and is a way for businesses to work with governments, which are ultimately responsible for upholding human rights commitments on a global level and monitoring compliance to these activities. Moreover, UNGC corporate participants commit to annual "Communications on Progress" (COP) that are made public by the UNGC. The format of the COP is flexible and allows companies to incorporate it into their general communications processes. Nokia's corporate responsibility reporting and COP can be found at: <http://www.nokia.com/corporate-responsibility/ethics/reports>.

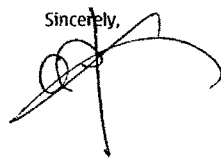
Nokia views the GNI as a well-intentioned group whose principles and implementation guidelines are generally consistent our own policies and practices. However, in our view the GNI is currently structured to narrowly address issues that arise for Internet service companies rather than technology and hardware companies and the private sector in general. Given our existing internal policies and practices in the area of human rights, as well as our ongoing involvement in well-established global organizations with parallel agendas, at this time we will continue to monitor the development of the GNI and are of course willing to continue in the dialogue about the critically important issue of the protection and promotion of human rights such as freedom of expression and privacy.

NOKIA

4

I thank you once again for the opportunity to provide Nokia's views on this matter. If you have further questions or need additional information, please contact Leo Fitzsimon, the head of Nokia's Washington, DC office, at leo.fitzsimon@nokia.com, or by phone at (202) 887-0145.

Sincerely,



Attachment: Nokia Code of Conduct

Nokia Code of Conduct

Setting the highest standards

Nokia has always recognized that its own long-term interests and those of its various stakeholders depend on strict adherence to applicable regulation, the Rule of Law and on following the highest standards of ethics. For Nokia, ethical business conduct does not mean mere minimum legal compliance. As an industry leader, we aspire to be among the best in the world in corporate responsibility, actively promoting human rights and environmental protection through our products and solutions. At Nokia this is everyone's responsibility and an integral part of managing Nokia's business and brand.

Nokia Group Executive Board has approved and issued this Code of Conduct, and it is shared and reinforced throughout the company. The Board periodically reviews this Code and follows its implementation closely.

The Nokia Values are embedded in this Code. Every employee is expected to conduct himself or herself, and his or her business, in line with this Code without exception. Stricter guidelines or more detailed instructions may be appropriate for certain regions, countries or functions, but they must not contradict this Code.

Better communication leads to better life

Nokia will respect human dignity and promote human rights. Nokia recognizes, with the international community, that certain human rights should be considered fundamental and universal, based on accepted international conventions and practices, such as those of the United Nations' Universal Declaration of Human Rights.

Among those rights that Nokia views as fundamental and universal are: freedom from discrimination on any grounds; freedom from arbitrary detention, execution or torture; freedom of peaceful assembly and association; freedom of thought, conscience and religion; and freedom of opinion and expression.

Nokia's products and technologies contribute positively to human rights, to the environment and in the development of many societal areas. Nokia actively seeks business opportunities for innovative solutions that enhance people's lives and well-being.

High ethics means success

Nokia is strongly committed to the highest standards of ethical conduct and full compliance with all applicable national and international laws. This includes, for example, labor conditions, antitrust and promoting fair competition, prevention of bribery and corruption, good corporate governance, the protection and recognition of copyright, company assets and other forms of intellectual property.

Nokia places the safety in the intended use of its products and services and consumer rights at the forefront, and conducts its marketing in a responsible way.

Nokia respects the privacy and integrity of users of its products and services, and other stakeholders. We endeavor to adhere to strict standards when processing

political groups.

Nokia employees must not profit, nor assist others to profit, from opportunities that are discovered through the use of corporate information or position. Nokia employees must not use corporate assets for other than legitimate business or other authorized purposes. Nokia employees must also not engage in any activity which competes with the business of the company.

We and our partners

Nokia requires its business partners, subcontractors, or suppliers to comply with applicable laws and regulations. Nokia encourages its partners, subcontractors, or suppliers to strive beyond legal compliance in areas such as governance, human rights and the environment. Nokia incorporates ethical, social and environmental criteria in its procurement agreements and commits to monitoring the performance of its partners and to taking immediate and thorough remedial steps in cases where the ethical performance of its business partners comes into question.

Implementation

Nokia's compliance commitment in this Code extends to all matters, including decisions relating to trade, investment, subcontracting, supplying, business development, and in all other business and employment relationships. Nokia's approach to implementing this Code of Conduct is active, open and ethically sound. Although difficult questions of interpretation may arise, Nokia will do its utmost to resolve any identified ethical, legal, environmental, employment, and human rights issues consistent with this Code of Conduct.

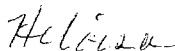
It is the responsibility of each Nokia employee to promote this Code of Conduct. The Nokia Ethics Office exists to support employees in all questions relating to this Code. Nokia employees are always encouraged, when possible and feasible, to raise questions and report issues relating to the Code of Conduct with their superiors. It is the responsibility of all Nokia superiors to support their teams in matters relating to the Code.

It is the responsibility of each Nokia employee to report on violations of this Code:

Nokia employees may report violations of the Code to their superior. It is the responsibility of all Nokia superiors to give advice on the proper procedure in case of violations.

Any issue involving a potential violation of the 'No tolerance of corruption' section in the Code, or any applicable legal rules or regulations, should be reported to the employee's Legal or Business Controller, with a copy being sent to the Assistant General Counsel. The Assistant General Counsel can also be contacted directly.

Furthermore, the employee may report an issue directly, confidentially and anonymously to the Nokia Board of Directors, its non-executive members or sub-committees through an electronic channel and a physical mailing address, both available on the company's website. In particular, issues related to Nokia's accounting, internal controls, or auditing matters are to be addressed to the Audit



1/4



August 27, 2009

Honorable Richard J. Durbin
Chairman, Subcommittee on Human Rights and the Law
United States Senate
Washington, D.C. 20510

Honorable Tom Coburn
Ranking Member, Subcommittee on Human Rights and the Law
United States Senate
Washington, D.C. 20510

Dear Chairman Durbin and Ranking Member Coburn:

I am writing in response to your letter of August 6th concerning Nokia Siemens Networks' approach to human rights issues, a topic that we take very seriously. In your letter, you request that we respond to a series of questions. I am pleased to share our responses below. First, let me give you an overview of our corporate philosophy, practices and commitments in this area.

Nokia Siemens Networks is a global telecommunications infrastructure supplier employing over 60,000 people in over 100 countries – including over 2,300 in the United States. We began operations in April 2007, a result of combining the network and carrier businesses of Nokia Corporation and Siemens Communications. While Nokia and Siemens are our parent companies, and our financial results are consolidated into Nokia, Nokia Siemens Networks is a separate and distinct legal entity. We provide hardware, software, and services to fixed and mobile telecommunications network operators.

Ours is a global and rapidly changing industry. In the mobile switching market, for example, the largest global market share is held by Huawei (32%), a Chinese company. Other major participants include Nokia Siemens Networks (22%), Ericsson (23%), and Alcatel-Lucent (8%), while the fastest growing new entrant is ZTE (1%), another Chinese company. Recently, the largest market participant based in North America, Nortel (5%), declared bankruptcy, and its operations are currently being auctioned off.

Nokia Siemens Networks shares your concern for the protection of human rights, including privacy and freedom of expression. As you noted in your letter, information and communications technologies (ICTs) are enabling billions of people around the world to express themselves by communicating with each other, offering their opinions, sharing ideas and even organizing around democratic beliefs in new and exciting ways. The global, interconnectedness of ICT networks transcends country and regional borders, bringing all of us closer together. Nokia Siemens Networks is extremely proud of the role we play in helping to make this possible.

Set out below are Nokia Siemens Networks' responses to the questions raised in your letter:

1. What are your company's views on the GNI?



Nokia Siemens Networks believes that the GNI is a promising effort to address concerns regarding privacy and freedom of expression. GNI's three core documents - Principles, Implementation Guidelines, and Governance, Accountability and Learning Framework - evidence a significant amount of thoughtful work.

The current list of GNI participants is an impressive coalition of civil society organizations, socially responsible investors, and academics, in combination with some ICT companies, notably Microsoft, Google, and Yahoo!. No telecommunications infrastructure suppliers are listed as participants in the GNI. As I explained above, we are in a very different business than Microsoft, Google, and Yahoo!. Our industry includes companies such as Huawei, Alcatel-Lucent, Ericsson, and ZTE. The industry does not provide services (e.g., Internet search, browsing) directly to individuals. While GNI is intended to be adaptable to the particular circumstances of a company, it seems to be focused on situations in which companies are holding large amounts of information about individuals that may be requested by governments or where the companies are delivering content directly to individuals that may be restricted by government measures. It is not clear that in its current form the GNI is well-adapted to the industry that Nokia Siemens Networks is in – the business-to-business supply of telecommunications infrastructure and services.

Given GNI's launch in 2008, it is not surprising that there is limited information on the application of GNI core documents to the operations of any of the current GNI corporate participants. Thus, Nokia Siemens Networks is unable to comment on the efficacy and value of the GNI commitments, either on their own or in comparison to similar obligations or principles to which a company has committed itself.

2. Will your company consider joining the GNI? If yes, please describe the process you will follow to consider joining the GNI. If no, why not?

Nokia Siemens Networks is prepared to further explore the possibility of joining the GNI. At a minimum, our assessment of the GNI will require a thorough analysis of its applicability to our business, its relationship to our existing code of conduct and other policies and initiatives (described below), the degree to which the GNI processes and procedures align with the scale and scope of its objectives, whether the principles are relevant to a broad range of industries and nations, and the impact of its implementation across the major companies in our marketplace.

To be effective in the long run, the GNI or any similar effort must be adopted by a broad cross-section of the global industry in question. It will not be effective if it has the effect of conferring competitive advantage on companies that may not operate in a manner consistent with human rights principles. In short, for a program like GNI to be successful, it needs a broad and truly global constituency. For example, the United Nations Global Compact (UNGC) includes over 5200 participants from 130 countries representing all industrial sectors committed to following its human rights principles. Both of our corporate parents, Nokia and Siemens, are long time signatories to the UNGC.



In sum, Nokia Siemens Networks is committed to maintaining a comprehensive approach to these issues that best combines effective internal policies, guidelines and procedures with involvement in the most pertinent external programs and organizations.

3. Does your company currently follow any of the GNI principles?

Yes, and they are deeply engrained in our core company values. Nokia Siemens Networks recognizes that its own long-term interests and those of its various stakeholders depend on compliance with the highest standards of ethical conduct and applicable law. Even before the start of our company in 2007, we made it clear that ethical business behavior and corporate citizenship would be an essential part of our culture and would need to be reflected in our daily work.

As part of this effort, we launched our Code of Conduct on the first day of the new company. The Code, updated most recently in January 2009, is designed to provide guidance on how to behave in different business situations and provides clear messages about where the boundaries lie between business that is appropriate and that which is not.

As stated, in part, under the heading "Better communication leads to better life" in the Nokia Siemens Networks Code of Conduct:

Nokia Siemens Networks will respect human dignity and promote human rights. Nokia Siemens Networks recognizes, with the international community, that certain human rights should be considered fundamental and universal, based on accepted international conventions and practices, such as those of the United Nations' Universal Declaration of Human Rights.

Among those rights that Nokia Siemens Networks views as fundamental and universal are: freedom from discrimination on any grounds; freedom from arbitrary detention, execution or torture; freedom of peaceful assembly and association; freedom of thought, conscience and religion; and freedom of opinion and expression.

Nokia Siemens Networks' products and technologies contribute positively to human rights, to the environment and in the development of many societal areas. Nokia Siemens Networks actively seeks business opportunities for innovative solutions that enhance people's lives and well-being.

4. Please describe your company's policies and practices for advancing and protecting human rights and minimizing the risk that your products and/or services will facilitate human rights abuses.

As noted above, the Nokia Siemens Networks Code of Conduct specifically addresses issues relating to the advancement and protection of human rights. It includes a pledge that Nokia Siemens Networks will do its utmost to resolve any identified ethical, legal, environmental, employment, and human rights issues so as to be consistent with the Code. We also require our business partners, subcontractors, and suppliers to comply with applicable laws and regulations and encourage them to



strive beyond legal compliance in areas such as governance, human rights and the environment.

The Code of Conduct has been approved by the Nokia Siemens Networks' executive board, as well as the company's board of directors, and is introduced and reinforced to Nokia Siemens Networks employees through induction, training and internal communications.

In addition, the Code of Conduct is administered by our Corporate Affairs group, whose head reports directly to me. The administration of the Code of Conduct includes training, the use of hotlines that allow for anonymous reporting and oversight by a Chief Ethics Officer. Moreover, when faced with business decisions, our employees can refer to internal experts in various areas for guidance, and escalate a decision to the Nokia Siemens Networks executive board when needed.

We would welcome the opportunity to meet with you to discuss these issues in greater detail. If you would like to arrange such a meeting or have further questions, I would ask you to contact Robert Weisberg, Head of Corporate Affairs for North America, at robert.weisberg@nsn.com, or Derek Khlopin, Head of Regulation and Policy for North America, at derek.khlopin@nsn.com, or either via phone at (202) 887-0145.

I appreciate your inquiry and the opportunity to explain how Nokia Siemens Networks supports and advances human rights.

Warmest regards,

A handwritten signature in black ink, appearing to read "Simon Beresford-Wylie".

Simon Beresford-Wylie
Chief Executive Officer
Nokia Siemens Networks

DICKSTEINSHAPIRO LLP

1825 Eye Street NW | Washington, DC 20006-5403
 TEL (202) 420-2200 | FAX (202) 420-2201 | dicksteinshapiro.com

August 27, 2009

Via E-mail and First-Class Mail

Chairman Richard J. Durbin
 Senator Thomas A. Coburn, Ranking Member
 Senate Committee on the Judiciary
 Subcommittee on Human Rights and the Law
 SD-224 Dirksen Senate Office Building
 Washington, DC 20510

Re: Global Network Initiative

Dear Chairman Durbin and Ranking Member Coburn:

I am writing on behalf of my client, McAfee, Inc. ("McAfee"), in response to your letter dated August 6, 2009. Below please find McAfee's responses to the questions posed in your letter concerning the Global Network Initiative ("GNI"). McAfee believes strongly in privacy and freedom of expression and appreciates your interest in these important issues.

By way of background, McAfee, headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee has more than 5,500 employees and has large sales/marketing and research organizations based in Colorado, Georgia, Minnesota, Oregon and Texas. McAfee is committed to relentlessly tackling the world's toughest security challenges. The company delivers proactive and proven solutions, services and global threat intelligence that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to comply with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. Much of McAfee's technical work supports the U.S. government, protecting such institutions as the Departments of Defense and Homeland Security, as well as various intelligence agencies.

1. What are your company's views on the GNI?

The GNI is a constructive and important step in the effort to raise awareness of, and expand the dialogue on, the impact of technology on human rights issues. McAfee supports GNI's stated purpose of encouraging companies to examine, as part of the regular strategic decision-making process, whether and to what extent their products and services may be used to limit freedom of expression and access to information.

Washington, DC | New York, NY | Los Angeles, CA

DICKSTEINSHAPIRO LLP

Chairman Richard J. Durbin
Ranking Member Thomas A. Coburn
August 27, 2009
Page 2

2. Will your company consider joining GNI? If yes, please describe the process you will follow to consider joining the GNI. If no, why not?

In light of your recent letter, McAfee is considering joining the GNI. To this end, McAfee is taking steps to understand more fully the principles, requirements, and ramifications of participating in the GNI, including discussions with current participants and GNI staff. We have begun a thorough review of all product lines; governance rules and processes from the perspective of human rights issues; relationships with partners; export control laws, systems and processes; and relevant domestic and international legal obligations. McAfee has also committed to attending a workshop hosted by GNI on September 10, 2009. At the conclusion of this process, McAfee will be far more knowledgeable and in a better position to determine the extent of its participation in the GNI.

3. Does your company currently follow any of the GNI principles?

McAfee believes that privacy and freedom of opinion and expression are fundamental human rights and guarantors of human dignity that should not be restricted by governments, except in narrowly defined circumstances. For instance, McAfee's SmartFilter® web filtering software, which was of particular interest to the Committee staff during a recent meeting, classifies Internet content into nearly 100 different categories so that customers can choose, by category, what types of web content they want made available to their organization. Although McAfee has no control over how an organization ultimately utilizes SmartFilter®, McAfee does not provide any categories that are intended to assist a user in discriminating on the basis of race, religion, political persuasion, gender, sexual orientation, or any other personal characteristics.

McAfee also believes in responsible company decision making, and, indeed, has begun the process of attempting to identify circumstances where freedom of expression and privacy may be further advanced or, from the opposite perspective, unwittingly jeopardized, and integrate these principles into its decision making.

DICKSTEINSHAPIRO_{LLP}

Chairman Richard J. Durbin
Ranking Member Thomas A. Coburn
August 27, 2009
Page 3

4. Please describe your company's policies and practices for advancing and protecting human rights and minimizing the risk that your products and/or services will facilitate human rights abuses.

As noted above, McAfee does not provide, as part of its SmartFilter® web filtering software, any categories that are intended to assist a user in discriminating on the basis of race, religion, political persuasion, gender, sexual orientation, or any other personal characteristics.

McAfee's Employee Handbook and Code of Business Conduct also emphasize the importance of privacy and confidentiality. The relevant portion of the Employee Handbook, for example, states in part: "Use of personal information may be subject to legal restrictions, and also may be subject to specific preferences and/or requirements requested by the customer, partner, and/or supplier. Respecting expressed privacy preferences and requirements is important to our competitive position in the industry, and in certain geographies it is required by law." The Code of Business Conduct provides: "Directors, officers and employees must maintain the confidentiality of confidential information entrusted to them by the Company, its customers, partners, distributors and suppliers, except when disclosures are specifically authorized by the Legal Department or required by law."

McAfee has strong export control systems and processes designed to ensure that none of its product is exported or re-exported to any country embargoed by the United States, including Cuba, Iran, Syria, North Korea, and Sudan, which are some of the most repressive regimes in the world.

As it has been reviewing its policies and practices with respect to the issues raised in the Subcommittee's letter, McAfee is willing to consider ways to make them more robust. McAfee will certainly consider addressing human rights issues explicitly in a company policy, such as the Code of Business Conduct. Moreover, McAfee is developing and will implement in 2010 a set of human rights assessment guidelines to inform its strategic business decision-making.

DICKSTEINSHAPIROLLP

Chairman Richard J. Durbin
Ranking Member Thomas A. Coburn
August 27, 2009
Page 4

Please do not hesitate to contact me at (202) 420-3447 if you have any questions. McAfee officials would also be willing to meet with you or your staffs to discuss these issues in greater detail.

Sincerely,



Mark R. Paoletta
(202) 420-3447
paolettam@dicksteinshapiro.com

PETER LOESCHER
PRESIDENT AND CHIEF EXECUTIVE OFFICER
SIEMENS AG

The Honorable Dick Durbin
Chairman
Subcommittee on Human Rights and the Law
Committee on the Judiciary
U.S. Senate
Washington, D.C. 20510

The Honorable Tom Coburn
Ranking Member
Subcommittee on Human Rights and the Law
U.S. Senate
Washington, D.C. 20510

September 2, 2009

Dear Chairman Durbin and Ranking Member Coburn:

Thank you for your letter of August 6, 2009, in which you discuss the human rights challenges facing information and communications technology (ICT) companies and encourage Siemens to join the Global Network Initiative. We appreciate your desire to improve companies' consideration of human rights factors when they make business decisions.

Siemens is active in 190 countries in the areas of Industry, Energy and Healthcare. Historically, ICT was a core Siemens business. However, as Siemens refined its business strategy, we decided to exit the ICT industry. Although Siemens no longer has operational or managerial control of any ICT business, I do want to assure you and members of the Human Rights and the Law Subcommittee that, as a matter of course, we make a conscious effort in our global operations to give something back to the local communities and participate in corporate outreach efforts.

With regard to the human rights issues raised in your letter, I have asked Peter Solmssen, who is the Member of the Siemens Managing Board responsible for Siemens compliance programs and with regional responsibility for the Americas, to provide you with a detailed description of the policies and practices Siemens has put in place.

Again, thank you for your interest in Siemens. I commend the Subcommittee for its endeavors to raise critical human rights issues and trust that our response addresses your concerns.

Sincerely,



Postal Address
Siemens AG

Office Address
Siemens AG

7-9 15 00 80 00 00 00

PETER Y. SOLMSEN
EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL
SIEMENS AG

Wittelsbacherplatz 2
80333 Munich
Phone: +49 (089) 636-39880
Fax: +49 (089) 636-39884
peter.solmssen@siemens.com

The Honorable Dick Durbin
Chairman
Subcommittee on Human Rights and the Law
Committee on the Judiciary
U.S. Senate
Washington, D.C. 20510

The Honorable Tom Coburn
Ranking Member
Subcommittee on Human Rights and the Law
U.S. Senate
Washington, D.C. 20510

September 2, 2009

Dear Chairman Durbin and Ranking Member Coburn:

Peter Loescher has asked me to respond in greater detail to the questions you raise in your letter of August 6, particularly with respect to Siemens' principles and business conduct guidelines.

As a global company, Siemens promotes issues such as sustainability and human rights as part of its corporate responsibility initiatives and business conduct principles. Siemens' business conduct guidelines mirror the human rights principles incorporated in the Global Network Initiative (GNI); and, due to our broad business portfolio and global reach, our principles extend beyond those of the GNI in a very real sense. Complying with our guidelines is mandatory for all Siemens employees and our business partners. Siemens' "Business Conduct Guidelines" call for respect for the dignity, privacy and personal rights of every human being. (cf. Section A.2). Siemens is also committed firmly to the UN Global Compact's ten principles. (Principles 1 and 2 re. Human Rights; cf. appendix to revised Business Conduct Guidelines).

Our company has participated in the United Nations Global Compact since 2003, and we adhere to the Universal Declaration of Human Rights and follow other international conventions and recommendations. Siemens provides whistle-blowing channels to all stakeholders, which may also be used to report suspected human rights violations (helpdesk, "Tell Us" and ombudsman). We actively collaborate with global non-governmental organizations (NGOs) in supporting broad policies to improve Siemens' role as a responsible global citizen. Last year, Siemens was rated "very high" on the Dow Jones Sustainability Index.

In addition to these commitments, Siemens supports the work of John Ruggie, United Nations Special Representative of the Secretary General (SRSG) on Human Rights, who has observer status with the GNI. We applaud the SRSG's concept of the state duty to protect and the responsibility of companies to respect human rights, including the duty not to become complicit in human rights violations (as stated in the UN Global Compact's principles). We also expect our business partners to respect human rights (section B. 8 and appendix to Business Conduct Guidelines and Code of Conduct for Siemens suppliers containing mandatory contractual requirements). Affiliated companies are obliged to apply the same policies and rules. Siemens also encourages its portfolio companies under external management control to adopt similar policies and rules in accordance with their respective portfolio and type of business. For more information, please go to: www.siemens.com/responsibility and the Siemens Sustainability Report, 2008, www.siemens.com/sustainability-report.

To provide you with further background material, I would add that Siemens sold its information and communications businesses and now has *no operational control over any company offering communications equipment*. Our relationship with companies offering these products can be generally characterized as an investor. Additionally, despite media reports to the contrary, cellular phone equipment sold to Iran by one of these companies did not contain any surveillance capability beyond what has come to be the worldwide standard, as the company has repeatedly stated.

Siemens' commitment to improving global conditions through its innovative products is clear, and as I just noted, we factor human rights considerations into our business decisions through our business conduct guidelines. Moreover, we work everyday with NGOs, respected international organizations and local communities across the globe to bring solutions that will improve people's lives. Therefore, we feel strongly that we already have the policies in place that respect human dignity and sustainability. We greatly appreciate the work of the GNI, but our business is not ICT-focused.

I hope I have adequately responded to your query to Peter Loescher and detailed clearly our position on our business activities as they relate to human rights. We support your efforts to ensure that business decisions are carried out responsibly. If you would like additional information about our efforts outlined above, please contact Kathleen Ambrose, Senior Vice President, Government Affairs, in Washington at 202-434-4800.

Sincerely,



Encl.: Siemens Business Conduct Guidelines



August 26, 2009

Senator Richard J. Durbin, Chairman
 Senator Tom Coburn, Ranking Member
 U.S. Senate Committee on the Judiciary
 Subcommittee on Human Rights and the Law
 224 Dirksen Senate Office Building
 Washington, D.C. 20510

Dear Chairman Durbin and Ranking Member Coburn:

Thank you for your recent letter regarding the Global Network Initiative (GNI) and on-going efforts by the technology industry to protect and safeguard freedom of expression and privacy across the globe. As a global company, Skype shares your concerns about the efforts of governments to violate core privacy rights and we appreciate the opportunity to discuss these important issues with you. Skype's answers to the specific questions you pose in your letter are set forth below.

I passionately believe in Skype's mission to enable the world's conversations. As you recognize in your letter, Skype has enabled billions of people around the world to express themselves more fully and freely. Allowing the world to communicate for free empowers and links people and communities everywhere. Our challenge is to provide our software to people all over the globe, including in Internet restricting countries, while being transparent to our users and staying within the boundaries of the local laws. We are committed to meet this challenge. How we achieve that goal -- as part of GNI or some other set of best practices that may be more tailored to the needs of companies in Skype's stage of development -- is something we are considering at Skype. It is our hope that the on-going dialogue between Skype, the current GNI members, and your offices will lead to constructive clarifications of the GNI governing documents that will enable Skype's participation in the initiative.

We agree with your assessment that every ICT company should take reasonable measures to minimize the risk of complicity with repressive governments who seek to restrict their citizens' ability to exercise their right to freedom of expression. There are complex moral, legal and regulatory issues associated with Internet companies providing their valuable tools in these Internet restricting countries. This maxim is true whether we are examining the need for and structure of regulating legislation such as the Global Online Freedom Act or the adoption of industry best practices to govern company behavior in this complex environment. We can all agree that the ability to responsibly provide these

Skype Communications S.à r.l.
 6ème étage, 22-24 Boulevard Royal, L-2449 Luxembourg, Grand-Duché de Luxembourg t +352 2653 9130 f +352 2653 9050
 Registration no. RC Luxembourg 9801466



Internet tools is critical for enabling free expression and innovation to people across the globe.

As you may be aware, Skype was founded as a Luxembourg company approximately six years ago. Skype is engaging with the Council of Europe (CoE) regarding its on-going efforts to facilitate practical ways for European companies to comply with the European Convention on Human Rights, including Article 10, protecting the right to freedom of expression, which is enforced by the European Court of Human Rights. You will, no doubt, be aware that the United States Government achieved full observer status at the CoE in 1996. Skype is an organizing participant in an upcoming European Dialogue on Internet Governance (EuroDIG), which is facilitated by the Council of Europe, and will have a strong emphasis on human rights and privacy. Skype has proposed that the current members of GNI participate in the September EuroDig event to encourage greater dialogue between GNI and COE and organize an adjacent meeting between current GNI members and potential new members to address specific issues facing small and European companies such as Skype.

To address your specific questions:

1. First, in your letter you ask about our "company's views on the GNI." Skype is supportive of the principles upon which GNI is founded and we strive to incorporate these principles and ideals in our daily business practices and larger decisions regarding market entry, product development, and other business initiatives. Moreover, we share your view that "GNI has great potential to advance and protect human rights," and believe that collaboration toward industry standards is the right way to proceed. Accordingly, we are undertaking due diligence to decide whether GNI is the appropriate entity to guide Skype as our business scales and more and more people use Skype across the globe. We agree with your assessment that the GNI Implementation Guidelines and Accountability Framework should be sufficiently adaptable to the particular circumstances of companies from all sectors of the ICT industry, regardless of size and geographic location. In fact, we are actively considering GNI membership and, as described above, have embarked in earnest discussions with current GNI members to agree upon modifications or clarifications to the governing documents that are necessary to facilitate Skype compliance with the GNI best practices.

2. Consistent with these discussions, you ask: "Will your company consider joining the GNI? If yes, please describe the process you will follow to consider joining the GNI. If no, why not? There are a number of factors Skype is considering as we evaluate GNI membership. These include, as discussed above, our current efforts to balance competing or overlapping requirements in multiple jurisdictions across the globe, as well as our desire to understand thoroughly the

impact on our business operations associated with GNI membership. We do not take the responsibilities associated with membership in GNI lightly and will join only after appropriate due diligence, which can be time consuming. The founding members of GNI negotiated for over two years to agree upon its governing documents. Although Skype was not party to the original negotiations, since the launch announcement last fall, we have engaged in on-going discussions about our possible participation in GNI with GNI's leadership, the CoE and industry participants.

As noted above, one area of concern for Skype is that the governing documents were created by three of the major U.S. Internet brands. Skype is a relatively young company, embarking on an initial public offering sometime in 2010 to separate from our parent company, eBay Inc. Our employee base, while growing, remains very small in comparison to the three founders of GNI. It is well understood that small businesses and entrepreneurs operate differently from larger businesses, and that small businesses bear a disproportionate share of the burden of regulation, whether the regulation is imposed by governments, or self-imposed by industry organizations and voluntary best practices. As the members of GNI have recognized, it is critical that the governing documents are sufficiently flexible to enable compliance by a range of companies regardless of their corporate structure or business mission.

The importance of recognizing Skype as a small business is relevant to your question regarding the process Skype will follow to consider joining GNI. To reiterate, Skype is fully supportive of the GNI Principles and is striving to incorporate those principles in our current business practices. There are, however, several aspects of the Implementation Guidelines and Accountability Framework that would have a significant impact on the resources of a small company such as Skype. For example, requirements that member companies develop written materials, including procedures for compliance and detailed annual reports for use by independent auditors will be difficult to implement on a timely basis given our current resources. Moreover, it is reasonable to assume that meaningful participation in an annual audit of business practices and experiences in making the Principles operational would require a significant time commitment from the employees tasked with overseeing implementation. Tasking these employees with this responsibility would necessitate a shift away from daily business activities crucial to serving our users towards meeting some of the more labor intensive and time consuming procedural requirements of GNI. Extending the compliance period for the written requirements and annual audits for small businesses or reducing the amount of bureaucracy involved would go a long way toward encouraging broader participation in GNI by small businesses as well as facilitating self-governance in these matters.

In addition, as part of the human rights impact assessment, the Implementation Guidelines require the review of policies, procedures and activities of potential partners. It must be acknowledged that often local law requires that communications products such as voice services are offered through local providers. For instance, in China, TOM Online, a Hong Kong based company with substantial local operations and assets, is the majority partner in our joint venture that brings Skype to Chinese residents. The software is distributed in China by TOM and TOM, just like any other communications company in China, has established procedures to meet local laws and regulations, including text filtering. These regulations include the requirement to monitor and block instant messages containing certain words deemed "offensive" by the Chinese authorities. I note that this only applies to the localized version of Skype. Skype makes available a Mandarin-version of our software which is not subject to the text filtering I discussed above. We believe that the content of Skype-to-Skype voice or video conversations are still secure and private. In other words, the issues highlighted in recent reports do not affect communications where all parties are using standard Skype software. They refer only to instant messaging communication in which one or more parties are using the co-branded TOM-Skype client software. Although Skype has little to no influence over TOM policies and procedures, we are able to uphold the principles of GNI by simultaneously offering the Mandarin version of our software. While none of these circumstances prevents a GNI participant from fulfilling its obligations under the Implementation Guidelines, and we recognize and appreciate the "best efforts" guidance incorporated into the guidelines, the limitation on the influence of small companies on enterprises in Internet-restricting countries, especially where local law and practicalities necessitates such partnerships, bears repeating.

Additional requirements such as incorporating freedom of expression and privacy compliance into assurance processes to ensure compliance with the procedures laid out in the Principles will require training of Skype's engineers and software developers. The requirement also necessitates adoption of procedures to facilitate incorporation of mechanisms to protect these universally recognized human rights into new software, technology, and products. As with the other Implementation Guidelines mentioned in this letter, given Skype's available resources, full compliance with this requirement could take additional time beyond the two years allotted in Phase One of the Accountability and Learning document.

While I have outlined several specific requirements set out in the GNI governing documents, modification or clarification of which could facilitate participation by small companies such as Skype, I believe that continued cooperation between the current GNI members and potential new members is the primary tool necessary to ensure a full understanding of the obligations of GNI membership and the potential modifications or clarifications that might be entertained by the current

membership. To date, Skype has had several productive conversations with GNI members and plans to continue our review of the governing documents with these members to facilitate agreement on provisions of the Implementation Guidelines that can either be clarified or modified. It is important to continue this dialogue and to include other small companies that are more similarly situated to Skype. Skype's proposal to organize a meeting in conjunction with the EuroDIG event scheduled in Geneva for this fall is simply one in a series of necessary conversations. We also note that the GNI members recently issued an invitation to all recipients of your letter to an "Open House" to discuss how its principles and guidelines are adaptable to different business models within the ICT sector. It is our hope that these meetings will result in concrete proposals for clarifications and modifications to the GNI guidelines to meet the needs of small businesses.

3. Next you ask in your letter whether "[our] company currently follows any of the GNI principles." As stated previously, Skype is supportive of the principles that are the foundation of the GNI documents. Skype incorporates these principles and ideals in our business practices by responsibly engaging with local governments, our users, and other stakeholders to advance freedom of expression and privacy globally. As in other areas of Skype's policy conformity efforts, we strive to deliver on policymakers' desires by minimizing multiple, overlapping jurisdictional mandates. Thus, as a Luxembourg established company, our primary efforts to protect free speech and privacy rights for the Skype user community have been based on European initiatives that seek to enshrine the same or similar principles as GNI.

I am proud of Skype's efforts to enable our users to have safe and secure voice conversations via Skype. As you noted in your letter, the recent circumstances in Iran where opposition protesters' were able to use the Internet and applications such as Skype to engage in free expression are an inspiring example of the benefits brought by ICT companies to citizens around the world. One way in which Skype follows the GNI principles is that we do not employ technologies such as Deep Packet Inspection (DPI) that can sift vast amounts of information travelling over the Internet in a manner that would compromise the privacy rights of our users. In fact, Skype goes to great lengths to ensure that our user's conversations are safe and secure. We only employ encryption and obfuscation technologies to defeat -- not enable -- such illegal eavesdropping. Notably, all Skype-to-Skype conversations -- voice, video, instant messaging, file transfer -- utilizing the standard Skype software are fully encrypted, and thus secure and private. Moreover, we embrace the principles through responsible company decision making and by incorporating the fundamental tenets of free expression and the right to privacy in our business practices, as described in our response to question 4 below.

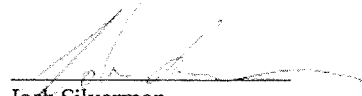
4. Finally, you request we “describe [our] company’s policies and practices for advancing and protecting human rights and minimizing the risk that [our] products and/or services will facilitate human rights abuses.” As stated previously, Skype is continually improving our business operations to protect and safeguard freedom of expression and privacy while ensuring that our users can continue to access the Skype software and communicate across the globe. Specifically, Skype:

- gathers and retains only minimal personal information about our users thereby minimizing risk should a security breach occur;
- has recently appointed a new Chief Information Security officer who is responsible for security policy development and management;
- is working to ensure that we are clear and transparent to our users about possible compromises in the security integrity of communications when the software is a version provided by a third party, including a complete overhaul of Skype’s security and privacy web pages;
- has established clear procedures for engaging with law enforcement authorities across the globe in accordance with Luxembourg law; and
- provides a Mandarin-version of our software which is not subject to the text filtering that is required by the Chinese government for the localized version of the software, distributed by our local partner TOM.

In addition to these precautions, as stated previously, all Skype-to-Skype conversations utilizing the standard Skype software are fully encrypted, and thus secure and private. The GNI requirements notwithstanding, Skype is conscious of the need for transparency, consistency and honesty in how we address the issue of the right to freedom of expression and privacy. In fact, given our mission to enable the world’s conversations, we are keenly aware that our users likely have a high expectation that we will protect their privacy and freedom of expression. We currently fulfill these obligations through the encryption and privacy protections that are built into the Skype software, and note that these protections are superior to those offered by traditional telecommunications firm operating in China or across the globe.

Thank you again for your thoughtful letter. Skype is committed to ensuring that users of communications and information technology tools across the globe are not stymied by threats to privacy and freedom of expression. We must all work together, governments and industry alike, to ensure that the Internet continues to be a tool for free expression, democracy and innovation. We look forward to continuing this productive dialogue with your office, GNI members and the COE.

Respectfully,



Josh Silverman
President

SKYPE COMMUNICATIONS S.A.R.L.
6e etage, 22/24 boulevard Royal,
Luxembourg, L-2449 LUXEMBOURG

Sprint

Vonya B. McCann
Vice President
Government Affairs

Sprint Nextel
Suite 700
900 Seventh Street, N.W.
Washington, D.C. 20001

August 27, 2009

The Honorable Richard J. Durbin, Chairman
The Honorable Tom Coburn, Ranking Member
Subcommittee on Human Rights and the Law
Senate Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senators:

Thank you for your letter of August 6, 2009 inquiring about Sprint Nextel Corporation's ("Sprint") possible participation in the Global Network Initiative ("GNI"). Sprint fully supports the laudable goals and objectives of the GNI. Every citizen of the world should enjoy the rights to freedom of expression and privacy without undue restriction or interference.

Sprint, however, does not typically confront the human rights issues that the GNI seeks to address, given the nature and scope of its network operations overseas. Outside of the United States, Sprint has deployed an Internet Protocol ("IP") wireline network in countries where the type of freedom of expression and privacy issues over which the GNI is concerned do not normally arise. Moreover, within such countries, Sprint's business is generally limited to providing private IP communications network services to U.S.-based multinational companies, which use our services to link their U.S. and foreign offices together. Sprint does not offer Internet access service to individual foreign end users located within those countries. Against that backdrop, below please find responses to your specific questions.

(1) What are your company's views on the GNI?

Sprint endorses the GNI's vision of promoting the rights to freedom of expression and privacy worldwide in the face of unwarranted government intrusion. Sprint commends the extraordinary commitment of the GNI's multi-stakeholder participants in developing a roadmap to help the ICT industry navigate through the difficult challenges such matters can present. The GNI's collaborative, self-regulatory approach, working in conjunction with U.S. government efforts, appears to be an effective way to advance global respect for human rights.

Office: (202) 585-1902 Fax: (404) 649-9286

The Honorable Richard J. Durbin, Chairman
The Honorable Tom Coburn, Ranking Member
August 27, 2009
Page 2

(2) Will your company consider joining the GNI? If yes, please describe the process you will follow to consider joining the GNI. If no, why not?

Sprint is in the process of reviewing and evaluating the details of the GNI. We intend to collect more information about the GNI and conduct an internal assessment of its application to Sprint. As part of that effort, Sprint representatives plan to attend the GNI Open House Discussion on September 10th for more information. Subject to further evaluation, Sprint may consider participating if it begins to confront these issues in the normal course of its international business operations. In the meantime, Sprint looks forward to closely monitoring the GNI's continued progress and engaging with GNI participants for more information.

(3) Does your company currently follow any of the GNI principles?

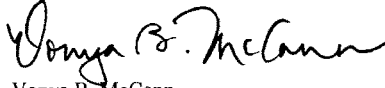
Sprint respects the fundamental principles of freedom of expression and privacy. Sprint seeks to ensure that its users' freedom of expression is not improperly restricted. Furthermore, Sprint is committed to protecting the privacy of the personal information it collects and disclosing such information only as required by law. We have privacy policies in place governing how we collect, access, use, disclose, and secure personal information both within and outside of the United States. Our Office of Privacy ensures implementation and compliance with our privacy program. For more information, please see: <http://www.sprint.com/legal/privacy.html> and <http://www.sprintworldwide.com/english/privacy.html>.

(4) Please describe your company's policies and procedures for advancing and protecting human rights and minimizing the risk that your products and/or services will facilitate human rights abuses.

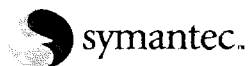
Given the current nature and scope of Sprint's international network operations discussed above, Sprint does not generally encounter human rights-related issues, and thus has no formal policies and procedures expressly dedicated to such matters other than those mentioned above. Should such issues arise, Sprint would seek to address them in a way that promotes the rights to freedom of expression and privacy and would look to the GNI as a key resource for guidance.

Thank you again for your inquiry.

Sincerely,



Vonya B. McCann
Vice President, Government Affairs



January 20, 2010

The Honorable Richard J. Durbin, Chairman
The Honorable Tom Coburn, Ranking Member
U.S. Senate Committee on the Judiciary
Subcommittee on Human Rights and the Law
United States Senate
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Durbin and Ranking Member Coburn:

I am responding to your letter subsequent to a meeting between Symantec and staff from the Senate Judiciary Human Rights and the Law Subcommittee regarding your interest that our firm participate in the Global Network Initiative (GNI). I would like to specifically respond to the questions raised in your letter in an effort to update you on Symantec's current human rights commitment.

Please be advised that Symantec does support the underlying purpose of the GNI- the protection and advancement of human rights including freedom of expression and privacy in the Information and Communications Technology (ICT) sector. We currently follow many aspects of the GNI principles and we are assessing the GNI indicators and considering what participating in the GNI on a formal basis would entail for our company. We are specifically evaluating the internal governance and accountability processes and procedures required under the GNI.

Symantec has a strong commitment to human rights and has made a public commitment to the Universal Declaration of Human Rights through the adoption of our Human Rights Policy Statement:

Human Rights Policy Statement

Symantec supports and respects the protection of internationally recognized human rights and labor standards proclaimed under the Universal Declaration of Human Rights and the International Labor Organization's core conventions. Our commitment to the realization of human rights is embedded in the company's Code of Conduct. Symantec respects the dignity of others and expects our employees and vendors to comply with the policies outlined in the company's Code of Conduct, local and international laws. We are a signatory to the United Nations Global Compact (UNGC) and encourage our suppliers to adhere to the UNGC's ten principles. Symantec's Board of Directors, Nominating and Governance Committee, have responsibility for oversight of the company's corporate responsibility effort which includes the Human Rights Policy.

In addition, Symantec has put the protection of our customers' privacy as a top priority. We have a comprehensive and transparent privacy policy in place, so that customers can choose what information to share with Symantec and how that information is used.

We will continue to do our due diligence and review of a more formal participation in the GNI including adoption of the principles. We are encouraged by the progress made by ICT companies to date, not only in their adoption of the GNI but in their willingness to come together collaboratively to protect and advance freedom of expression and privacy. We look forward to continuing to engage in this dialogue.

Should you have any additional questions regarding Symantec's Human Rights Policy efforts please feel free to contact me or Cecily Joseph with our Corporate Responsibility office at (650) 527-5058 or cecily_joseph@symantec.com or Kevin Richards of our U.S. Federal Government Relations office at (202) 429-7122 or kevin_richards@symantec.com.

Thank you for reaching out to Symantec to discuss the Global Network Initiative.

Sincerely,

A handwritten signature in black ink, appearing to read 'ES Salem', written in a cursive style.

Enrique Salem
Chief Executive Officer

Kathryn C. Brown
 Senior Vice President
 Public Policy Development &
 Corporate Responsibility



1300 I Street, N.W., Suite 400 West
 Washington, DC 20005

Phone 202 515-2407
 Fax 202 336-7914
kathryn.c.brown@verizon.com

August 27, 2009

The Honorable Richard J. Durbin
 Chairman
 U.S. Senate Committee on the Judiciary
 Subcommittee on Human Rights and the Law
 224 Dirksen Senate Office Building
 Washington, DC 20510

The Honorable Tom Coburn
 U.S. Senate Committee on the Judiciary
 Subcommittee on Human Rights and the Law
 224 Dirksen Senate Office Building
 Washington, DC 20510

Dear Chairman Durbin and Ranking Member Coburn:

Thank you for your letter of August 6, 2009 to Mr. Seidenberg regarding the role of the Global Network Initiative (GNI) and issues regarding the protection of human rights. He has asked me to respond on behalf of Verizon. We commend your leadership around these issues as Chairman and Ranking Member of the Human Rights and the Law Subcommittee and note the significant achievements of your subcommittee in advancing human rights internationally. As a responsible corporate citizen, Verizon shares a deep commitment to respecting those rights, and we were pleased to have had the opportunity recently to meet with staff from the Subcommittee about Verizon's approach to human rights issues. Your letter similarly seeks our views on the GNI and its principles, and our policies and practices for advancing and protecting human rights.

Our commitment to protect human rights is expressed in our corporate policies and practices, which, we note, cover the topics of freedom of expression and privacy that the GNI principles also address. Our Statement on Human Rights (<http://responsibility.verizon.com/home/approach/human-rights>) underscores our commitment to promoting the human rights values embedded in our Commitment & Values and Codes of Conduct. That statement cross-references the principles of the United Nations Universal Declaration of Human Rights, including freedom of expression. Our Privacy Principles (<http://www.verizon.com/privacy/>) and our Guiding Principles for Content on Verizon Networks (www.verizon.com/contentpolicy) set forth our policies on customer privacy.

While applauding the objectives of the drafters of the GNI, we note that their businesses and experiences in other nations are markedly different from Verizon's. As a result, we find this document to be problematic in several areas. As you note, Verizon was not among the companies included in the development of the GNI, and the GNI's provisions

The Honorable Richard J. Durbin
The Honorable Tom Coburn

August 27, 2009

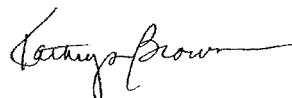
Page Two

do not reflect our circumstances as a global network service provider with assets, employees, and local facilities and operations subject to local licensing and other laws in many parts of the world.

Verizon recognizes the challenges the Subcommittee faces in developing effective measures to address international human rights violations, including those related to freedom of expression. Be assured that Verizon is committed to the goal of promoting human rights values and to being a positive force in society wherever we do business. While, as you recognize, the GNI may be one avenue for reducing exposure to human rights violations for its participating companies, it may make sense to explore with a broader set of businesses a different approach to a statement of principles that could be generally applicable and widely supported. An effective and inclusive statement should recognize the value of differing ways to achieve the shared objectives, including policies such as ours outlined above, and promote the critical role for government-to-government responses when abusive policies exist. For example, the strong actions by the Department of State and the U.S. Trade Representative have been widely credited with helping to prompt the decision by the Government of China to withdraw requirements to pre-install restrictive software on computers. Verizon would welcome a process for engagement in the development of a statement of principles on this important issue with a broad set of businesses and other stakeholders.

We appreciate this opportunity to share our perspective and would like to work with you and your staff to further address these issues.

Sincerely,



Kathryn C. Brown
Sr. Vice President
Public Policy Development &
Corporate Responsibility

Vittorio Colao
Group Chief Executive



27 August 2009

Senators Richard J. Durbin & Tom Coburn
United States Senate
Washington
DC, 20510
USA

Dear Senators Durbin and Coburn

Thank you for your letter of the 6 August concerning the Global Network Initiative.

I share your conviction that mobile communications is a powerful agent for empowering citizens and facilitating freedom of communication and expression. Vodafone already provides such opportunities to over 300 million people worldwide and we expect to extend those to many others in the future.

I am always mindful of the responsibilities that Vodafone has to the communities we serve. Vodafone has always been committed to the principles of free expression and concerned to protect the rights and interests of our customers. This is why, for example, we have Group-wide privacy policies which are applied in each of the companies under our direct control. Vodafone is also a minority shareholder in a number of companies where we engage actively with our partners on these issues.

Vodafone was an early participant in the dialogue which helped create the GNI. We found this process very valuable and it has shaped our own thinking on these issues. We did not to sign up to the GNI principles at launch because, unlike many internet service providers, Vodafone is also subject to national laws and regulations with which we must comply if we are to operate the network infrastructure and use the radio spectrum we need if we are to deliver mobile services in a national market. We will, however, continue to engage with the GNI and with other external stakeholders on these issues in the pursuit of our shared objectives of free expression and human rights. We are fully committed to full public disclosure of our position on these and other issues, further details of which you can find in our latest reports at www.vodafone.com/responsibility.

Yours sincerely

A handwritten signature in black ink, appearing to read "V. Colao".

Vittorio Colao

Vodafone Group Plc

Vodafone House, The Connection, Newbury, Berkshire RG14 2FN, England
Telephone: +44 (1635) 664 194, Facsimile: +44 (0)1635 676 109

Registered Office: Vodafone House, The Connection, Newbury, Berkshire RG14 2FN, England. Registered in England No. 1833679

Websense responses to questionnaire from Senator Durbin regarding the Global Network Initiative and human rights issues

What are your company's views on the GNI?

Websense believes that GNI and similar initiatives are extremely important because they highlight the issues raised when well-intended products are abused by oppressive regimes in a manner that compromise fundamental human rights. Corporations need to better address how oppressive governments may use their products as a tool to limit freedom of expression and thought, and public consumers need to actively motivate the corporations who sell these products to focus on corporate responsibility regarding human rights and worldwide censorship issues. We believe the principles in GNI are right on the mark and Websense already manages our business in accordance with them. We hope that the GNI can encourage companies across our industry to abide by GNI's principles.

Would your company consider joining the GNI?

Yes, Websense would consider joining the GNI because of the importance of the initiative in driving public and corporate awareness of the problem. However, as a small company we are concerned about the high costs associated with participation in the GNI in terms of up-front participation fees as well as the ongoing administration burden, particularly since we already manage our business consistent with GNI's principles. Websense General Counsel Mike Newman will contact GNI to discuss the company's concerns.

Does your company currently follow any of the GNI principles?

Yes, Websense already follows all of the principles of the GNI.

Please describe your company's policies and practices for advancing and protecting human rights and minimizing the risk that your products and or services will facilitate human rights abuses?

Our goal as a company has always been to create a solution that protects organizations and their employees from unwanted and malicious content on the Internet, whether it's Web-based malware or simply content that is inappropriate in the workplace. Websense products have never been designed nor intended to be used as a tool by governments to oppress or censor people's private Internet use. Earlier in our company's history we did not have an official anti-censorship policy in place, but we discouraged business if we felt it wasn't in line with the company's mission and culture.

As global Internet use has risen exponentially in emerging markets, it's become increasingly apparent that certain governments intend to implement solutions like ours in ways that are not consistent with our corporate objectives or values. To clarify our position and to dispel rumors that Websense sells products to governments and government-controlled ISPs that use our products to restrict Internet access and content for their citizens, we created a social responsibility policy relating to anti-censorship that is implemented globally. The policy is posted on our Web site, with similar language contained in every contract that our customers and our channel partners sign:

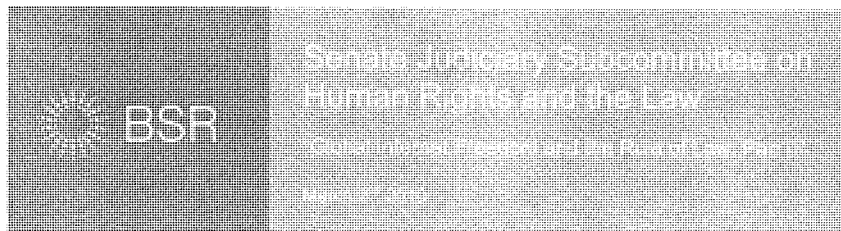
"Websense does not sell to governments or Internet Service Providers (ISPs) that are engaged in any sort of government-imposed censorship. Any government-mandated censorship projects will not be engaged by Websense. If Websense does win a business

and later discovers that the government is requiring all of its national ISPs to engage in censorship of the Web and Web content, we will remove our technology and capabilities from the project. Websense does however, provide filtering services in response to "global filtering" projects where the government mandated policy (1) prohibits minors from accessing pornography and/or (2) prohibits child pornography. With the above guidelines in place an example scenario would be if a government wants to prevent minors from seeing pornography at the ISP level. If that government then requires all ISPs to block adult content from all users, but permits an adult user to gain access to that content after providing proof of age, then this is a project that Websense can participate in. Websense, however, does not engage in any arrangements with foreign governments (or government-imposed arrangements) that could be viewed as oppressive of rights."

Many U.S.-based companies – Websense competitors – actively pursue business with governments that use the technology to filter private citizens' Web use, but we don't participate in that kind of business. The purpose of our Web filtering and Web security products is to make the Internet a safer place to do business, ensuring security and organizational productivity, while limiting legal liability for employers.

We do a good job of avoiding entering into any business arrangements that are contrary to our policy, but because we sell globally through more than 1,000 resellers to more than 40,000 customers, on rare occasion things can slip through the cracks. For example, we recently learned that two ISPs in Yemen were using our solutions not in accordance with our policy. When an unusual circumstance like the Yemeni ISP situation occurs, we conduct an investigation, gather information and provide the customer in question an opportunity to come into compliance with Websense terms, conditions and policies. If they choose not to, we take steps to suspend or terminate the customer's product subscription – as we did in the case of the Yemeni ISPs. To be completely transparent on this topic, we even publish our investigation and review process on our Web site.

The only government-sponsored Internet filtering projects we participate in are those where a government policy prohibits child pornography and/or prohibits minors from accessing pornography. We believe these projects are consistent with our corporate objective of making cyberspace a safer place to be.



Business for Social Responsibility (BSR) welcomes the opportunity to discuss issues of technology and human rights with the Senate Judiciary Subcommittee on Human Rights and the Law. Information and Communications Technology (ICT) has been one of the most powerful drivers of change in our global society and will increasingly shape how we protect and advance human rights today. For this reason we are pleased by the increased attention being paid to the interrelationship between ICT and human rights. This is a topic of relevance in all countries around the world, as governments everywhere seek to understand how to maintain legal frameworks and law enforcement efforts that are consistent with the human rights of freedom of expression and privacy.

BSR is a non-profit organization working with its global network of more than 250 member companies to develop sustainable business through advice, research, and cross-sector collaboration. With six offices in Asia, Europe, and North America, we use our expertise in the environment, human rights, economic development, and governance and accountability to guide global companies toward creating a just and sustainable world. BSR works with a diverse range of ICT companies including internet, software, semiconductor, telecommunications, consumer electronics and equipment manufacturing companies on a wide range of corporate responsibility topics, including human rights. In various capacities we have been partnered with the participants in the Global Network Initiative (GNI) on internet freedom issues since late 2005.

Introduction

This written submission is based upon our broad experience working with companies on human rights issues across a range of industries. The key question for the ICT industry as a whole and its stakeholders is this: "how can we design future ICT networks to minimize risks to human rights at every stage of the ICT value chain, and maximize the human rights potential of new technology?" We emphasize three main points for the Senate Judiciary Committee on Human Rights and the Law to keep in mind during its deliberations:

1. The relationship between ICT and human rights is complex and requires the active engagement of companies across the whole ICT industry, not just internet companies.
 2. Integrating human rights considerations into decisions about market entry and market exit will lead to different conclusions in different circumstances.
 3. There is a need for the whole ICT industry and its stakeholders to integrate human rights principles into their decision making, with processes tailored to the specific needs of the ICT industry.
- 1. The relationship between ICT and human rights is complex and requires the active engagement of companies across the whole ICT industry, not just internet companies.**

BSR has promoted integration of human rights principles into business decisions by advising companies in multiple industry sectors, and by working on collaborative multi-stakeholder solutions since 1995. Concerted efforts to apply human rights principles in the ICT sector are a more recent phenomenon, and in our view, present various unique features:



BSR

- » Compared to other industries where human rights impacts are often location specific, the end user is more significant: ICT products and services bring unique human rights risks and opportunities for billions of end users across multiple jurisdictions.
- » Technology often moves faster than the law: the regulatory process tends to move more slowly than ICT product and service development.
- » ICT functionality is introduced rapidly: new products and services bring new risks and opportunities all the time, often with unpredictable consequences.
- » Technology is complex to understand: there is only a very small community of stakeholders who fully understand the human rights implications of ICT.
- » For a wide range of reasons, governments often take great interest in the interrelation of human rights and ICT.

These factors point to the need for in-depth, constructive and collaborative efforts that bring together companies, governments and stakeholders to understand the unfolding relationship between human rights and ICT, especially as technology, data and online communications become increasingly pervasive. It is particularly important that these efforts delve deeply into the human rights implications of specific ICT products, services and functionalities and remain open to the idea that ICT brings both risks and opportunities.

For example, the common assumption is often that internet and telecommunications companies (such as Yahoo!, Google and Microsoft that participate in the GNI) are in the frontline on human rights in the ICT industry. However, it is our view that human rights risks and opportunities can exist at every stage in the ICT value chain – equipment manufacturers, consumer electronics companies and software firms, for example – and it is only by considering the ICT industry as one whole ecosystem that human rights can be most effectively protected.

For instance, telecommunications equipment and handset manufacturers design the product functionalities that enable law enforcement, including intercept, surveillance and location identification, while software companies build and maintain vast IT infrastructures for the storage, analysis, and processing of data which can be used for good or for ill.

These factors also indicate the need for significant government-to-government dialogue on these issues. In particular, governments around the world need to reach a shared understanding of how to maintain legal frameworks and law enforcement efforts that are consistent with the human rights of freedom of expression and privacy, and put in place approaches that enable ICT companies to more easily operate around the world in a manner consistent with human rights.

2. Integrating human rights considerations into decisions about market entry and market exit will lead to different conclusions in different circumstances.

Google's recent announcement to reconsider its business in China has won considerable praise, but it will be some time before we know whether the company's approach has a positive or negative impact on freedom of expression. However, the company's decision to cite human rights as a reason for potentially leaving China raises much broader ethical questions about the role of human rights in corporate decisions to enter or exit a market.

Is it always right to leave a country on human rights grounds? It is our view that while leaving can sometimes be the right approach, there will also be cases where companies should stay and engage, seeking to make a positive impact on human rights while they are there.

When it comes to determining whether a company's decision to enter or exit a market is good or bad for human rights, there's no one-size-fits-all rule, and the merits of the decision will vary considerably with the context—including the types of products and services the company has on offer, the relationships the company has in the country concerned, and the ability of the company to influence human rights in a positive direction.



As such, "are you in or are you out" may be the wrong question. No company automatically advances human rights by leaving a country, and, likewise, no company automatically improves the situation by staying. In all but the worst cases, it's *how* business participates in challenging markets that is the ultimate test. Does the company have a clear understanding of how its products, services, and market presence will impact human rights? Has the company identified its most significant human rights risks, and does it understand how to mitigate them? Is it working with sympathetic government partners to advance human rights?

It is also perfectly reasonable to expect that two companies may look at the same set of facts and reach different conclusions about which approach will be most effective in advancing human rights: Just as one company may decide that leaving is the best route to advance human rights, so another may decide that staying and engaging is the more impactful route. Maybe we need both.

Whatever one's opinion about market entry and exit, the fact that an increasing number of companies are weighing these decisions demonstrates that human rights considerations are reaching senior leaders in business like never before. We believe it is right to applaud companies that seek to integrate human rights into their decision-making, to criticize those that don't—and to be open to the fact that this could mean praising both companies that seek to make an impact by staying in difficult markets as well as those that decide to leave.

3. There is a need for the whole ICT industry and its stakeholders to integrate human rights principles into their decision making, with processes tailored to the specific needs of the ICT industry.

In this written submission we have communicated two main messages, that the interaction between ICT and human rights is complex, and integration of human rights considerations market entry and market exit decisions may result in different decisions for different companies in different circumstances.

These two beliefs lead us to a third conclusion: that there is a need understand further how to integrate human rights principles into business decision making in a manner that is tailored to the specific questions relevant to the ICT industry.

A number of excellent human rights due diligence tools have been created in recent years, such as those maintained by the Danish Institute of Human Rights and the International Business Leaders Forum, as well as by BSR. However, it is our opinion that the next step is for these and other similar tools to be thoroughly tested, refined and built upon by ICT companies from across the sector by using them in real life situations. This may include, for example, questions about product design, development and functionality, market entry and exit, and a determination of where selling to particular customers create significant risks of human rights violations.

We also believe that in the coming years the ICT industry as a whole will need to understand how the forthcoming business and human rights framework resulting from the work of John Ruggie, the UN Special Representative of the United Nations Secretary-General on business & human rights, can be most effectively applied to the sector.

Conclusion

We live in an age where ICT, data and information are increasingly pervasive, and this trend will only accelerate. This transformation brings with it new risks and opportunities that will require much greater literacy on human rights from those working in business and much greater literacy in ICT by those working outside of the industry. That will only happen when multiple parties come together in the pursuit of shared learning and collaboration for shared goals. We must also remember that the difficult questions being considered by the Committee are by no means unique to any single country. They are relevant in multiple jurisdictions around the world. We hope that the Committee is successful in stimulating the global, industry wide and multi-stakeholder dialogue that is required on these important topics.



Computer & Communications Industry Association

Written Statement of Edward J. Black
President & CEO, Computer & Communications Industry Association
 Before the Senate Judiciary Subcommittee on Human Rights and the Law
Global Internet Freedom: Corporate Responsibility and the Rule of Law
 March 2, 2010

The Computer & Communications Industry Association (CCIA) has been a longtime advocate of 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 Internet's ability 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.

We are here today partly because of the high profile battle of a major technology company in China. But the number of companies and countries impacted are far greater. There are few easy answers as companies try to bring their technology services and communications tools into nations that have different rules about privacy, free speech and freedom of expression.

Without the backing of their own government, companies often are faced with the unappealing decision to follow local laws or exit the market. Companies are working alongside government and human rights groups to support Internet freedom. The Global Network Initiative (GNI) is a collaborative project begun in 2009 in which a handful of American companies, including Microsoft, Google and Yahoo!, participate with international human rights organizations and academics.

Ultimately, however, countries – not companies – must battle countries on trade and human rights issues. We appreciate recent actions by the U.S. State Department on censorship and the Commerce Department and the United States Trade Representative on Internet filtering software. We need a greater, holistic commitment to use existing human rights agreements and trade laws to support a free, open Internet.

To respond to government crackdowns on protesters while looking away when a government cracks down on access to the open Internet sends a signal that we are not serious about Internet freedom. The U.S. government must consistently treat Internet freedom as a human rights issue and a trade issue in its dealings and communications with foreign governments.

While I now represent a wide variety of technology and communication companies, freedom of expression as a human rights and trade issue is a topic I have cared deeply about throughout my career. I was honored to served in the State and Commerce Departments under five Secretaries in the 1970's, and early 80's, where I worked on East-West trade and was actively involved in the approval of the first U.S./China trade agreement. I later chaired and still serve on the State Department's Advisory Committee on International Communication and Information Policy.

900 Seventeenth Street NW Suite 1100 Washington, DC 20006 Tel: 202.783.0070 Fax: 202.783.0534

In my experience, we may not get very far lecturing the Chinese government about human rights, but treating Internet censorship as a trade barrier is a multilateral approach worth pursuing. The EU Parliament voted in 2007 to recognize Internet censorship as a trade barrier. The USTR could engage its European counterparts to jointly explore how Internet censorship by the Chinese government functions as a trade barrier, and bring an appropriate case before the WTO.

U.S. companies are leading vendors of information products and services. In this context, information discrimination fundamentally undermines market access for electronic commerce. When the Chinese government stifles online freedom for its citizens, it creates a hostile market environment by preventing them from fully using new products, applications and services offered by or through U.S. tech companies. In this context, censorship is a protectionist industrial policy as well as an information control policy.

Moreover, the Chinese government's actions seem to constitute violations of its WTO-GATT obligations, as well as specifically scheduled commitments in relation to GATS and China's WTO Accession Protocol. The WTO is a viable forum because it represents a global rules-based trade system that China, as the world's largest exporter and the world's most export-driven economy, must appear to respect.

Aside from bringing a WTO action against China, the U.S. government should:

1. Establish a Special 301-like process for the USTR to annually review to place on a watch list those U.S. trading partners which perpetuate the most egregious acts or practices of censorship that affect trade, and review the trade privileges of those trading partners whose attacks on Internet freedom impair U.S. enterprise and threaten U.S. jobs. If U.S. corporate content production is worthy of such a process, so too must be U.S. enterprise that depends on freedom of expression.
2. Highlight Internet censorship policies in trade reports on China.
3. Initiate multilateral consultations to ensure we are participating in the family of nations adhering to the Universal Declaration of Human Rights – in particular, Articles 19 (freedom of expression) and 20 (freedom of assembly), which in the 21st century must include the “freedom to connect.”
4. Actively support the Global Network Initiative (GNI).

The Chinese government needs to understand that access to its markets is not a coin that enables them to buy their way out of respecting human rights and freedom. Countries that have supported China's growth as a world player in the belief that its economic growth would lead to it becoming a “responsible stakeholder” need to object when the Chinese government's unreasonable demands on issues like Internet censorship prove inconsistent with such responsibility. Nations that support freedom of expression must elevate Internet freedom to the top of their human rights and trade agenda.



1534 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Written Submission of the Center for Democracy & Technology

Before the Senate Judiciary Committee,
Subcommittee on Human Rights and the Law

GLOBAL INTERNET FREEDOM AND THE RULE OF LAW II

March 2, 2010

Chairman Durbin, Ranking Member Coburn, and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to submit this written statement. We applaud the Subcommittee's leadership and continued attention to corporate responsibility and Internet freedom.

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. However, the challenges to global Internet freedom have only grown more complex and difficult since this Subcommittee's hearing in 2008 on the issue.¹ Authoritarian regimes are increasingly enlisting companies and the technologies they produce to remake the Internet into a tool of political control. Last year, China asked computer manufacturers to pre-install the Green Dam filtering software on all computers sold in China in an attempt to further decentralize its censorship regime.² Many governments are increasingly building up surveillance and censorship capabilities using technologies developed in the west.³ And authoritarian regimes are becoming ever more sophisticated in using new media technologies to propagate their own messages and control online debate.⁴

Just as important, many of our democratic allies are taking actions in the name of addressing various social ills that also jeopardize the environment for expression and innovation on the Internet. An Italian court just convicted three Google employees for a video posted by a user under the theory that might force companies to review all user-

¹ For our previous testimony to this Committee on this issue, see *Global Internet Freedom: Corporate Responsibility and the Rule of Law: Hearing before the Senate Judiciary Comm. Subcomm. on Human Rights and the Law*, 110th Cong. (2008) (statement of Leslie Harris, President & CEO, Center for Democracy & Technology), <http://www.cdt.org/testimony/testimony-leslie-harris-global-internet-freedom-corporate-responsibility-and-rule-law>.

² OpenNet Initiative Bulletin, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," OpenNet Initiative, July 27, 2009, <http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc>.

³ See, e.g., Heidi Noman, "Middle East Censors Use Western Technologies to Block Viruses and Free Speech," OpenNet Initiative Blog, <http://opennet.net/blog/2009/07/middle-east-censors-use-western-technologies-block-viruses-and-free-speech>; Naomi Klein, "China's All-Seeing Eye," Rolling Stone, May 29, 2008, http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye/print.

⁴ *Global Internet Freedom: Corporate Responsibility and the Rule of Law II: Hearing before the Senate Judiciary Comm. Subcomm. on Human Rights and the Law*, 111th Cong. (2010) (statement of Rebecca MacKinnon, Visiting Fellow, Princeton University), http://conversation.blogs.com/files/rm_slc_2march2010.pdf.

generated content before it can be hosted on their services in Italy.⁵ In an overbroad claim of jurisdiction, Belgium authorities have ignored existing treaties and imposed fines on Yahoo! for refusing to hand over user data.⁶ And Australia is advancing a mandatory Web filtering proposal that requires ISPs to implement a secret government blacklist for prohibited content (an approach that is of questionable efficacy in fighting child exploitation).⁷ Authoritarian regimes often point to such actions by democratic governments to justify their own acts of censorship and surveillance.⁸

Advancing Global Internet Freedom Requires Action on Multiple Fronts

The Internet has developed and flourished because of a policy framework based on competition, openness, innovation, and trust. That framework puts power not in the hands of centralized gatekeepers but in users and innovators at the edges of the network. It protects intermediaries such as ISPs and Web hosts from liability for content created by their users. And this framework minimizes government interference. Under this approach, the Internet is able to fulfill its potential as an engine of democratization, economic growth and human development.

However, as the above examples illustrate, this policy framework is under threat globally and U.S. leadership and advocacy is urgently needed worldwide. Secretary of State Clinton's landmark speech in January 2010 elevated global Internet freedom high on the foreign policy agenda of the United States. Clinton's speech should be a starting point for a broad and sustained effort by the U.S. government to keep the Internet open, innovative and free. To implement the Secretary's vision, CDT urges the U.S. government to take action in four areas:

1. Guard Internet freedom at home
2. Advocate for Internet freedom through all the tools of diplomacy, trade, and foreign aid at the government's disposal
3. Support Internet activists all over the world
4. Promote and support corporate social responsibility in the ICT sector

Companies, Congress, and a wide range of U.S. governmental actors can play a key role in advancing efforts in all four areas.

⁵ Thomas Claburn, "Google Execs Convicted in Italy," *Information Week*, February 24, 2010, http://www.informationweek.com/news/hardware/utility_anddemand/showArticle.jhtml?articleID=223100801. See also, Leslie Harris, "Deep Impact: Italy's Conviction of Google Execs Threatens Global Internet Freedom," *Huffington Post*, February 24, 2010, http://www.huffingtonpost.com/leslie-harris/deep-impact-italys-convic_b_474648.html.

⁶ Cynthia Wong, "Yahoo! protects user privacy -- and gets fined?", *Policy Beta Blog*, July 11, 2009, <http://www.cdt.org/blogs/cynthia-wong/yahoo-protects-user-privacy-and-gets-fined>.

⁷ Andrew McDiarmid, "Filtering Down Under," *Policy Beta Blog*, December 18, 2009, <http://www.cdt.org/blogs/andrew-mcdiarmid/filtering-down-under>.

⁸ See, e.g., Leslie Harris, "21st Century Statecraft: the Internet as Diplomat," *Ahead of the Curve*, ABC, <http://abcnews.go.com/Technology/AheadoftheCurve/Internet-diplomat-21st-century-statecraft/story?id=9740416&page=3> (quoting a translated reaction from a Chinese official to Secretary of State Clinton's speech on Internet freedom).

Companies are key actors in keeping the Internet open and free

Governments hold the primary obligation to protect human rights, and one ultimate goal of any collective strategy to advance Internet freedom must be to change the behavior of Internet-restricting countries themselves. However, as the UN Special Representative on business and human rights John Ruggie has determined, while “their responsibilities cannot and should not mirror the duties of States,” companies have a responsibility to respect human rights.⁹ Secretary of State Clinton confirmed this notion in her speech in January, saying, “[t]he private sector has a shared responsibility to help safeguard free expression. And when their business dealings threaten to undermine this freedom, they need to consider what’s right, not simply what’s a quick profit.”¹⁰

Communications technologies and new media services have become vital to the lives of millions of users all over the world. We have seen extraordinary examples of the ability of these technologies to amplify voices and speak truth to power in Iran, Burma, and Tibet in the past two years. Just as important, these technologies offer new ways for citizens in all countries to come together, speak out on common concerns, and participate in their own governance. The products and services offered by even the smallest Internet start-up can be potentially reached by any user on the global Internet. But “[n]o matter where you live, people want to believe that what they put into the Internet is not going to be used against them.”¹¹ Just as good corporate citizens strive to minimize the environmental impact of their operations and prevent labor violations in its workforce, ICT companies must address the risks to freedom of expression and privacy raised by their business operations.

Exercise due diligence and avoid complicity in human rights violations

First and foremost, companies have a responsibility to avoid complicity in governmental acts of censorship and surveillance. John Ruggie has set forth a thoughtful framework for corporate responsibility that centers on the exercise of “due diligence,” which 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 proactive strategies to minimize human rights risk; and
- Ongoing monitoring and auditing to track performance and improve practices.¹²

As intermediaries between governments and citizens, technology companies will face increasing pressure from governments to implement Internet controls as a way of decentralizing state Internet repression. In addition, even if a company is merely offering

⁹ John Ruggie, *Protect, Respect and Remedy: a Framework for Business and Human Rights*, at 16-17 (April 7, 2008), <http://www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf>.

¹⁰ Secretary of State Hilary Rodham Clinton, Remarks on Internet Freedom, Newseum, Washington, DC, January 21, 2010, <http://www.state.gov/secretary/rm/2010/01/135519.htm>.

¹¹ Secretary of State Clinton, Remarks on Internet freedom, *supra* note 9.

¹² Ruggie report, *supra* note 8, at 17-19.

their product for sale, where technologies can be used for both good and bad, companies have a responsibility to mitigate the impact of foreseeable uses of their products by states that seek to transform ICTs into a tools of political control. Companies must exercise due diligence in anticipating and addressing these risks.

When governments enlist companies in acts of censorship and surveillance, companies have a range of options for how they respond, almost all of which will fall short of pulling out of a difficult market. Specific company decisions about what products and services to offer (and to what customers), how those products and services are designed, and how the company responds to government requests to take down user content or hand over user data can have an enormous impact on users' ability to speak and protect their privacy.

The Green Dam incident in 2009 and Google's announcement in January 2010 on its operations in China make clear that companies can no longer passively ignore the human rights risks that arise in the ICT sector or engage in unthinking adherence to local law.¹³ The ethical dilemmas are only going to get harder, and companies must have a thoughtful, systematic, and proactive approach in how they will respond, or else risk complicity in human rights violations and the loss of user trust in their business practices and products.

Promote practices that guard Internet freedom

Companies also have a responsibility to promote policies and practices by governments – at home and abroad – that guard Internet freedom. Governments all over the world are struggling to address longstanding social ills in the new digital era. But when governments seek to surveil without a warrant in the name of security, impose filtering mandates to protect children, or threaten to cut Internet access for users to enforce intellectual property laws, companies must make the case that the adoption of such policies in democratic countries make all the more difficult for them to operate responsibly elsewhere in the world. No market is without ethical risk, and the ICT sector has a clear role to play in advocating for governmental policies and practices that protect user rights all over the world, including at home.

Collaborate with stakeholders

The Global Network Initiative (GNI) provides a framework for companies to systematically examine and mitigate the human rights risks their businesses face in various countries. After extensive consultation, research, and benchmarking, the GNI produced a set of high-level Principles and detailed Implementation Guidelines that begin to develop a standard for corporate responsibility and human rights due diligence in the ICT sector. These Principles and Guidelines provide operational guidance for ethical company decision-making all around the world. GNI companies commit to implementing the Principles throughout their operations, conducting human rights risk assessments, and crafting strategies to mitigate risks presented – all with the help and support of human rights and technology policy experts, investors, and academics. The

¹³ Cynthia Wong, Deconstructing Green Dam, Policy Beta Blog, August 24, 2009, <http://www.cdt.org/blogs/cynthia-wong/deconstructing-green-dam>.

GNI also acts as a platform for collaboration on key issues of government policy and for collective action when emerging threats to Internet freedom arise. Companies strengthen their hand when they work with other companies and non-company stakeholders to push back against government demands that impact human rights.

Companies who join the GNI not only benefit from this framework for engagement and collaboration, but also more credibly demonstrate their commitment to addressing human rights risk by engaging in a transparent and accountable way.. To be clear, GNI's accountability mechanisms are not a "gotcha" exercise: The goal is to improve company processes and to enhance the Principles and Guidelines over time through a collaborative learning process..

In CDT's view, GNI offers the most promising path forward for companies to join with other key stakeholders to address the challenge of Internet freedom. While it may be possible for a company to find an alternative means of managing human rights risk, it is demonstrably clear that doing nothing is no longer an option.

Congress should promote corporate responsibility and support companies in managing human rights risks

Ensure companies are exercising human rights due diligence

Congress can play an important role in ensuring companies are acting responsibly. Congress should encourage industry adoption of the UN Special Representative Ruggie framework for corporate responsibility and exercise of human rights due diligence. Policymakers can support companies in conducting human rights impact assessments (HRIAs) by assisting efforts to craft tools and standards for assessing human rights risk in the ICT industry and to develop strategies for mitigating risk. Because GNI members have done extensive benchmarking on ICT-focused risks, Congress should encourage companies to join the GNI and take advantage of the collective expertise and real-time problem solving assistance that the GNI offers.

Congress can also encourage greater information sharing between companies and relevant government agencies around human rights challenges the ICT industry faces and how the industry is responding. Such exchange could help better inform development of policy and diplomatic strategies, as well as serve as a resource for companies striving to minimize human rights risks in their business. However, such data sharing must be implemented in a way that protects personal user information and does not introduce additional confidentiality concerns.

Finally, if Congress acts legislatively, we urge Congress to do so in a way that both incentivizes *and* supports responsible engagement by companies across the ICT industry. While CDT supports the goals of the Global Online Freedom Act of 2009 (GOFA) [H.R. 2271], the approach this legislation takes may be impractical in implementation and under-inclusive at best, and may do more harm than good at worst.¹⁴ GOFA does not address the roles and actions of a range of companies that

¹⁴ For CDT's analysis of a previous iteration of the Global Online Freedom Act [H.R. 275, 110th], see CDT, "Analysis of the Global Online Freedom Act of 2008 [H.R. 275]: Legislative Strategies to Advance Internet Free Expression and Privacy Around the World," May 2, 2008, <http://cdt.org/international/censorship/20080505gofa.pdf>.

provide hardware, software, and telecommunications products. In addition, the specific mandates that GOFA would place on delivery of Internet services in Internet restricting countries may even discourage provision of these vital platforms for expression.

Address the export of technologies to countries with a demonstrated history of Internet repression

Many of the most Internet-restrictive regimes use technology developed by American companies to implement their systems of censorship and surveillance.¹⁵ The companies at issue have had varying degrees of direct involvement in the sales, installation, consultation, and training associated with such governmental uses of their technologies.

Congress should direct an examination of whether narrowly targeted export restrictions are necessary for technology or related services that enable surveillance or censorship in countries with a demonstrated history of Internet repression (or where use of technologies or services to facilitate human rights violations is reasonably foreseeable). These restrictions should apply especially where technologies and services are specifically designed or customized to enable governmental censorship or surveillance in high-risk countries.

However, the U.S. government must also ensure our export policies do not chill free expression on the global Internet. Even some of the strictest sanctions provided by U.S. law carve out exceptions for information and information materials, or transactions involving books, journals, and newspapers.¹⁶ The goal of these exceptions is to support free expression and access to information in countries where discourse and media are tightly controlled. However, many of these regulations were passed before the advent of new media tools and user generated content services such as instant messaging clients, social networking sites, and even web hosting services. In the face of uncertainty about how these rules apply to new technologies (and threat of fines if a company missteps), companies may hesitate to offer communications technologies and platforms for speech to sanctioned countries¹⁷ – resulting in a policy misalignment that serves to undermine U.S. foreign policy goals around promoting human rights and democratic values.

We are encouraged by the Obama Administration's announcement this March to issue a general license for the export of many of these new media tools.¹⁸ CDT encourages Congress and the Administration to further examine other changes necessary to promote the use of tools by advocates in sanctioned countries that expand free expression and access to information, while also protecting user privacy.

¹⁵ See, e.g., Helmi Norman, "Middle East Censors Use Western Technologies to Block Viruses and Free Speech," OpenNet Initiative, July 27, 2009, <http://opennet.net/blog/2009/07/middle-east-censors-use-western-technologies-block-viruses-and-free-speech>; Rebecca MacKinnon, "More on Cisco in China," RConversation, June 30, 2005, http://conversation.blogs.com/rconversation/2005/06/more_on_cisco.html.

¹⁶ See, e.g., 31 C.F.R. § 560.210(c) and § 560.315 (exempting informational materials such as publications, films, posters, and news wire feeds from the Department of the Treasury, Office of Foreign Assets Control regulations on Iran).

¹⁷ See Eric Lai, "Should Facebook, Twitter follow IM providers and block access to U.S. 'enemies'?", Computerworld, June 10, 2009, http://www.computerworld.com/s/article/0134233/Should_Facebook_Twitter_follow_IM_providers_and_block_access_to_U_S_enemies_.

¹⁸ Mark Landler, "U.S. hopes Internet Exports will Help Open Closed Societies," New York Times, March 7, 2010, <http://www.nytimes.com/2010/03/08/world/08export.html?ref=technology>.

Support and equip companies to deal with government requests that violate human rights

While some argue that technology companies should simply withdraw from challenging markets, most Internet freedom advocates agree with CDT that the *responsible* engagement by the U.S. ICT industry in these markets – and the communications platforms, information services, software and hardware they provide – play an important role in expanding global Internet freedom. Many companies are struggling to find an ethical path forward, sometimes pushing back or finding ways to skirt the edges of vague censorship mandates, and other times stumbling badly and inadvertently facilitating human rights violations.¹⁹ A broad range of governmental actors can help support and equip companies striving to be instruments of Internet freedom all over the world:²⁰

- Support more extensive country reporting by the State Department on the legal, political, and policy environment for Internet freedom.
- Support training of officials and staff in the Department of State, Department of Commerce, the Office of the USTR, and other relevant agencies on global Internet freedom issues with the goal of enabling agency staff to aid companies and Internet advocates abroad, intervene where threats to Internet freedom arise, and integrate Internet freedom as a vital component of all American foreign policy.
- Encourage greater information sharing between government, industry, and NGOs about emerging human rights challenges. However, increased information sharing must be implemented in a way that protects user information and does not introduce new privacy concerns.

Provide technical support for Internet users and activists

As governments are becoming increasingly sophisticated in controlling information and silencing political dissent online, Internet users and activists in closed societies need a range of training, technology and support to counter novel means of control and the Internet policies that enable such control.²¹ Congress should:

- Fund dissemination of and training for a range of tools that enable circumvention of content controls and protect privacy across multiple platforms (web, wireless, mobile, etc.).
- Incentivize private sector development of technologies that enhance users' ability to circumvent content controls and protect their privacy.

¹⁹ See, e.g., Erica Naone, "Search Engines' Chinese Self-Censorship," *Ahead of the Curve*, ABC, July 1, 2008, <http://abcnews.go.com/Technology/AheadoftheCurve/story?id=5280133&page=1> and Nart Villeneuve, *Breaching Trust: An analysis of surveillance and security practices on China's TOM-Skype platform*, October 2008, <http://www.nartv.org/2008/10/01/breaching-trust-tom-skype/>.

²⁰ See also *Global Internet Freedom: Corporate Responsibility and the Rule of Law II: Hearing before the Senate Judiciary Comm. Subcomm. on Human Rights and the Law*, 111th Cong. (2010) (statement of Daniel J. Weitzner, Associate Administrator for Policy Analysis and Development, National Telecommunications and Information Administration, Department of Commerce).

²¹ Testimony of Rebecca MacKinnon, *supra* note 4.

- Fund efforts to support NGOs engaged in policy reform efforts in countries around the world. Creating and preserving a policy framework that supports openness and trust on communications networks is a vital underpinning to all Internet freedom efforts. Advocates need to build capacity to promote sound Internet policies, in addition to protesting censorship.

Ensure domestic policies set the right example abroad

Finally, Internet freedom begins at home and the U.S. must lead by example. The U.S. is facing a range of complex policy challenges, from cybersecurity to intellectual property to protecting children online. The policy solutions we adopt must also take Internet freedom goals into account, and these solutions should be crafted in an open and accountable way, subject to public debate. Finally, we must take care not to set precedents that can be used by authoritarian regimes to justify their own acts of censorship and surveillance.

In sum, the ICT industry and a range of U.S. governmental actors have vital roles to play to advance global Internet freedom and ensure communications technologies remain engines of democratization, economic growth, and human development. CDT applauds Senator Durbin, Senator Coburn, and the other members of the Subcommittee for their continued commitment to this issue. CDT looks forward to working with Congress on ways to keep the Internet open, innovative, and free.

##

For more information, please contact:

Leslie Harris, President & CEO
lharris@cdt.org
 (202) 637-9800 x115

Cynthia Wong, Ron Plesser Fellow
cynthia@cdt.org
 (202) 637-9800 x117



**Written Testimony for the Senate Judiciary Subcommittee on Human Rights and the Law on
"Global Internet Freedom and the Rule of Law, Part II"**

Committee to Protect Journalists

March 9, 2009

Internet companies play vital role in defending internet journalists

The Committee to Protect Journalists would like to thank the chairman and committee members for this opportunity to present our written testimony on the subject of global Internet freedom, the responsibility of corporations to promote and defend it, and the importance of the rule of law across the world.

When CPJ began in 1981, journalists at risk of reprisal for their work frequently had some element of institutional support. They were often employed as professionals by newspapers or other media companies. Their publishers and editors would stand by their employees, even as those journalists were harassed, imprisoned, or tortured.

Last year, for the first time, our research found that half of all journalists jailed around the world worked online. Most of them were freelancers or independent journalists with little or no institutional support.

Google, Yahoo, and other Internet companies are not publishers or the editors of their sites' content: their millions of users are. But we believe their actions play a profound role in today's media. These companies in effect provide the phone lines journalists use to gather news. They manage virtual newsstands and create online, public gathering places.

While the Internet has allowed people across the world to have their own virtual printing press, to publish without needing anyone else's permission, and to instantly speak to a potential audience of more than a billion people, it has also given us "information chokepoints"—a handful of companies and facilities that repressive governments use to silence users. Governments no longer have to shut down dozens of newspapers and individual radio stations. Now they can simply halt the circulation of information by pulling the plug on the Web. When they want to make pictures of Tiananmen Square protests vanish from the historical record, they need only force a few search engines to comply.

The responsibilities of Internet companies are not the same as those formed by the close relationship between traditional editors and publishers and their reporters. But we must all recognize the key role these companies play in freedom of expression across every modern state. We urge governments and the companies you have contacted (Amazon, Apple, AT&T, Cisco, Dell, eBay, Facebook, Fortinet, HP, IAC, IBM, Juniper, Lenovo, McAfee, Motorola Acer, News Corporation, Nokia, Nokia Siemens, Oracle, RIM, SAP, Siemens, Skype, Sprint Nextel, Toshiba, Twitter, Verizon, Vodafone, and Websense) to take steps to better defend the Internet freedom their own businesses, and the functioning of modern democratic society, now depend upon.

Below are our suggestions for action that we respectfully offer to those companies, and to the committee.

Companies must include at-risk journalists when considering user privacy

Companies should require due process when law enforcement seeks access to information, and minimize the data they collect. In January 2010, Google was alerted to the human rights implications of

a serious attack on its internal systems because the attackers sought out private information on Chinese activists held within the company

That shows that it is more urgent than ever that Internet companies pay close attention to the security of their users' data. Corporations should be encouraged to use encryption to protect personal data within their own systems, and SSL or other secure protocols to protect communications as they pass over the Internet.

But companies should also be wary of how information about their users can leak out in other ways. Just a few months after that deliberate attack, Google launched the social networking service Google Buzz, a new Twitter-like feature that inadvertently leaked out private information about who wrote to whom using their Gmail accounts.

The personal information that these companies work so hard to protect in one scenario may be revealed by their own subsequent business practices. Facebook recently changed its privacy policy, making it harder for its users to hide their list of friends from strangers. This was after *The Wall Street Journal* reported that the Iranian government was using Facebook to track and identify ex-patriot dissidents and connect them to vulnerable family and friends. By changing privacy settings universally, Google and Facebook risk handing information to those who seek to harm or discredit journalists, or to unmask their sources or identities.

The responsible course for companies whose services are used in repressive regimes is to include in their testing these new services a new category—along with “early adopter,” “power user,” “soccer mom” and “digital native”—that of “at-risk journalist” or “dissident author.” These are people who depend as much, and perhaps more so, on these companies' services, and deserve not to be put at risk by their decisions.

American companies must not collaborate in creating the tools of surveillance and censorship

All of the companies who have given testimony to the committee have contributed to the construction of an incredible instrument for free expression. The Internet that journalists use every day, in every country, has been built and improved upon by these companies' innovation.

But there is increasing revenue to be made by undermining that amazing tool, by building its opposite: software and hardware that enables Internet censorship and surveillance beyond the principles of due process and the rule of law.

We must ensure that American companies do not sell repressive countries the equipment for censorship. Corporations need to conduct human rights audits of their businesses in repressive regimes, and forbid their employees from offering consultation or providing services that directly contribute to government monitoring or control in countries where the rule of law and defense of human rights is weak or nonexistent.

If these companies fail to live up to these basic ethical standards, it may be necessary to enforce it through further regulation. But we must be cautious that well-meaning but overbroad sanctions or trade controls do not have the effect of preventing beneficial technological innovation from reaching journalists in the very worst conditions. The Treasury Department's March 8 announcement of the relaxing of sanctions in Cuba, Iran, and Sudan for personal Internet communication products and services is an important step forward in this regard. We hope the State Department will continue to regularly revisit the question of sanctions and how they affect local and international journalists who use American online services in these and other sanctioned countries. For the avoidance of liability, many companies continue to interpret sanction provisions broadly and may, for instance, block Internet addresses in sanctioned countries or even prohibit citizens from using their services at all. Clear

statements encouraging companies to support Internet communication in these countries and suggested terms-of-service language provided by the State or Treasury departments would encourage American companies to offer powerful tools for free speech in the very nations that need them most.

The fight for Internet freedom requires a united international approach

Secretary Clinton has said that making a principled stand on censorship should be part of America's national brand. With great respect to what we believe was a groundbreaking and compelling speech on Internet freedom, we believe a principled stand on censorship is an international standard, to which all countries and companies should adhere.

We firmly believe that companies' actions to defend freedom of expression and defend online journalists should not be seen as an arm of American foreign policy, but as an obligations to comply with the framework of international human rights laws. It is important that the international community support these actions. Our trade partners and allies can, and should be encouraged, to play their part in promoting the basic values of free expression and a free press that we all share.

Nonetheless, the United States can do more. Many companies that are not based in the U.S. nonetheless benefit from its financial and investment infrastructure. For instance, the Chinese search engine Baidu trades on the NASDAQ exchange, and recently benefited in a dramatic increase in its stock price after Google's January announcement that it would challenge China's requirement that it censor its local search results. It would be a travesty for American companies to rise to the challenge of defending Internet free expression and the work of online journalists only to have other global corporations, supported by American investment, undermine their work.



Written Testimony of Arvind Ganesan,
Director, Business and Human Rights Program,
Human Rights Watch:

Senate Committee on the Judiciary,
Subcommittee on Human Rights and the Law

March 8, 2010

**“Global Internet Freedom: Corporate
Responsibility, and the Rule of Law, Part II”**



Mr. Chairman, Senator Coburn, and members of the subcommittee,

Thank you for allowing Human Rights Watch the opportunity to submit written testimony on internet freedom, corporate responsibility, and the rule of law to the Senate Judiciary Subcommittee on Human Rights and the Law.

We would like to focus on two issues that we think are critical to securing greater respect for human rights online:

- The current status of voluntary efforts to ensure corporate responsibility, and other steps needed to ensure that companies respect human rights.
- The elements of a comprehensive and effective US policy to promote internet freedom.

Corporate Responsibility

The Global Network Initiative (GNI) was launched in October 2008, a few months after your first hearing on this subject. It is an important effort to safeguard freedom of expression and privacy on the internet by obliging member companies to adopt and implement human rights standards; to independently assess their compliance; and to provide a forum to collectively address challenges to freedom of expression and privacy online.

However, we believe that one of the key challenges today is the reluctance of companies to join the effort. The founding member companies, Google, Microsoft, and Yahoo, are the only companies currently in the GNI. No other companies have joined. We believe this problem is fundamentally a lack of political will on the part of companies and a failure to recognize their human rights responsibilities. The GNI's structure and governance is flexible enough to allow a wide variety of companies from the internet and telecommunications industries to adapt its principles to their operations. It has a phase-in period for implementation and monitoring that provides for three years between the time they join the GNI and the time when they will be fully assessed for compliance. And it has a progressive fee structure that currently begins at \$2,000 annually for a company with less than \$100 million a year in revenue to \$60,000 annually for a company with more than \$100 billion a year in revenue.

We welcome your committee's efforts to encourage companies to adopt human rights standards and your recognition of the GNI as an initiative to implement them. But the response of companies has been very disappointing. Their approach also stands in stark contrast to Secretary of State Clinton's January 22, 2010 speech. In that major address on internet freedom, she acknowledged the GNI and stated that "[c]ensorship should not be in any way accepted by any company from anywhere," and noted that "American companies need to make a principled stand." She also said that the "private sector has a shared responsibility to help safeguard free expression. And when their business dealings threaten to undermine this freedom, they need to consider what's right, not simply the prospect of quick profits."

We believe that this is a crucial moment for companies to demonstrate their commitment to human rights. For example, Google's announcement in January 2010 that it was prepared to leave China due to censorship and attacks on the privacy of human rights activists underscores how important it is for companies to adopt and embrace human rights policies and practices, such as those espoused by GNI.

However, as we noted in our testimony to the subcommittee in May 2008, voluntary standards are not enough. As we currently have seen with GNI, companies may not join them, and governments may be adept at dividing or pressuring companies to ignore voluntary efforts in favor of access to their markets.

For these and other reasons, we continue to believe that legislation is an essential step to complement efforts such as the GNI. As we remarked in our May 2008 testimony, new rules and regulations would 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. Legislation would also ensure 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 it could encourage a more assertive US foreign policy on these issues. In the wake of new developments, such as Secretary Clinton's speech and the passage of the Victims of Iranian Censorship (VOICE) Act in October 2009, this is an opportune time to examine legislation.

In the House of Representatives, House Speaker Nancy Pelosi noted on January 13, 2010 that "It is essential that technology companies not assist in efforts that violate human rights or prohibit the free exchange of ideas." Several other members have also proposed legislation to legally protect human rights online. These are important steps and we hope that

Congress will enact legislation to ensure that internet and telecommunications companies respect human rights.

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, which includes provisions for adequate due diligence, and can be 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 addressed through US diplomatic or other government-to-government 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.
- A restriction of access to federal funds for companies that do not abide by these standards.

Government Policy

In her January 22 speech, Secretary of State Clinton recognized that an open internet is not just a matter of human rights, but integral to economic development and political stability. For example, the most comprehensive search engines are offered by US companies. When

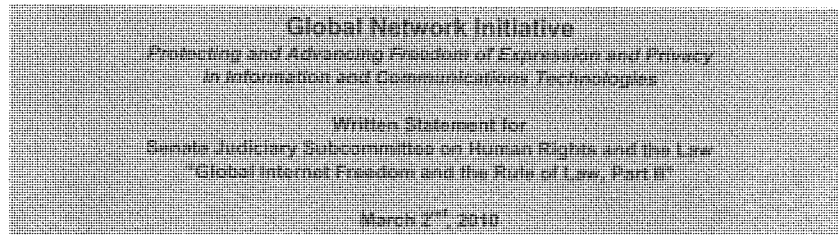
they have to censor in order to operate in foreign markets, they have to offer a lesser product, thus undermining their ability to fairly compete.

At a minimum, Human Rights Watch believes that the Obama administration should take the following steps to put these policies into practice:

- US diplomats should regularly press their counterparts to eliminate online censorship.
- The administration should ensure that all government agencies work to combat censorship through the establishment of a high-level office for internet freedom.
- The Commerce Department or the US Trade Representative (USTR) should call for an open internet in the course of commercial diplomacy and trade negotiations, for example. And future US trade agreements should have provisions to protect freedom of expression online, comparable to labor protections. This could include modifying Trade Promotion Authority to explicitly incorporate Freedom of Expression.
- The administration should also begin a formal review of US export control laws to better regulate certain technologies to ensure that governments do not use them to censor their critics.
- Expand reporting requirements such as those under the Victims of Iranian Censorship Act to more countries. That law requires the US government to issue reports to determine whether non-Iranian companies may have provided surveillance or censorship technologies to the Iranian government.
- Require companies to demonstrate that they have policies and procedures in place to protect human rights online as part of any government cooperation or support for their efforts.

We hope that the administration will take these steps on its own, but would welcome legislation to strengthen those efforts.

We believe that this is a critical moment to protect human rights online and we thank the Subcommittee for its leadership on the issue.



The Global Network Initiative (GNI) welcomes the opportunity to discuss internet freedom and the rule of law with the Senate Judiciary Subcommittee on Human Rights and the Law.

All over the world - from the Americas to Europe to the Middle East to Africa and Asia - companies in the ICT industry face increasing government pressure to comply with domestic laws and policies that require censorship and disclosure of personal information that conflict with internationally recognized human rights laws and standards.

In an effort to protect and advance the human rights of freedom of expression and privacy, a diverse coalition of leading information and communications technology (ICT) companies, major human rights organizations, academics and investors launched the GNI in October 2008.

The GNI is founded upon Principles on Freedom of Expression and Privacy and supported by specific implementation commitments and a framework for accountability and learning. Together, this framework provides a systematic approach for companies, NGOs, investors, academics and others to work together in resisting efforts by governments that enlist companies in acts of censorship and surveillance that violate international standards.

The Initiative is founded on the internationally recognized laws and standards for human rights on freedom of expression and privacy set out in the Universal Declaration of Human Rights ("UDHR"), the International Covenant on Civil and Political Rights ("ICCPR") and the International Covenant on Economic, Social and Cultural Rights ("ICESCR").

These three features – foundation upon international human rights standards, a multi-stakeholder approach and global applicability – underpin the unique value of the GNI. It is our belief that the organization has the potential to lead the way in helping companies make decisions that protect the freedom of expression and privacy rights of hundreds of millions of Internet users around the world. However, there are two inter-related issues that must be addressed if the GNI is to reach its full potential and maximize its positive impact on human rights:

1. While the GNI's top-level Principles are relevant across the whole ICT ecosystem – equipment manufacturers, software providers, search engines, consumer electronics companies and telecommunications services providers – there are business and human rights issues impacting this sector (such as sales of filtering software or surveillance equipment) that the GNI's Implementation Guidelines may not address. We need broad stakeholder input to fashion guidelines to incorporate these issues.
2. Even among Internet services companies for whom the existing Principles and Implementation Guidelines are on point, participation has not expanded beyond the original three US internet companies. Respect for internationally recognized rights of freedom of expression and privacy will most likely advance where a broad cross-section of companies makes this commitment, and so it is important that a much larger number of companies participate in the GNI's work.

1. GNI Implementation Dialogue – Drawing from the Whole ICT Ecosystem

The GNI Principles and Implementation Guidelines were drafted using a multi-stakeholder approach involving companies, investors, academics and NGOs. Among the companies were global internet and telecommunications firms and for this reason the content of the GNI's Principles and Implementation Guidelines reflects the specific circumstances faced by these companies.

While the top-level GNI Principles are relevant to firms across the ICT sector, we recognize that GNI's Implementation Guidelines require some adaptation or supplementation in order to more directly guide companies in other segments of the ICT industry, such as equipment manufacturers, consumer electronics brands, handset manufacturers and the providers of security and filtering services, enterprise management software and databases. The GNI has established an "Implementation Dialogue" to achieve this objective.

Since the launch of the GNI in October 2008 the organization has engaged in conversations with a wide variety of ICT companies including semiconductor manufacturers, software providers, equipment manufacturers, consumer electronics brands and telecommunications services providers. These conversations have tended to converge on three important questions:

- What do ICT companies view as their main privacy and freedom of expression risks and opportunities?
- What do these risks and opportunities reveal about the relevance of the existing GNI Principles and Implementation Guidelines?
- Can the existing GNI Implementation Guidelines be adapted or supplemented to increase their relevance to a wider range of ICT companies?

Despite the diversity of companies that together constitute the whole ICT industry, views about the relevance of the existing GNI Principles and Implementation Guidelines have been remarkably consistent.

First, and very importantly, there are large sections of the GNI documents that are entirely relevant to the whole ICT industry. This includes, for example, the top level Principles, and the commitments relating to responsible company decision making, human rights impact assessments and multi-stakeholder collaboration to advance human rights.

Second, there are four areas where GNI can take the lead in developing standards to increase the relevance of the Implementation Guidelines to a wider range of ICT companies. Here we set out these four interrelated questions in more detail and they will guide the GNI Implementation Dialogue to bring more companies into GNI.

i. Understanding freedom of expression and privacy risk associated with *product functionality*

The GNI's Implementation Guidelines are currently focused on the level of the *content* (e.g. circumstances in which a company should/ should not remove content) and at the level of *personal information* (e.g. circumstances in which a company should/ should not disclose personal information to law enforcement agencies).

However, to become relevant for a wider group of companies, we need to explore how the GNI documents may apply at the level of the *product functionality* – in other words, what impact the product functionality created by the ICT company can have on freedom of expression and privacy. One example would be how firms should respond if governments were to mandate the

installation of censorship capabilities in products, such as devices or software. Key questions include:

- What ability does an ICT company have to design or control the functionality of products to minimize censorship or illegitimate access to personal information? For example, this could include network equipment functionality that enables intercept and surveillance, or pre-installed products in consumer electronics such as filtering and surveillance software.
- Are there ways to design future ICT networks or create global product standards that will minimize risks to privacy and freedom of expression at every stage of the ICT value chain?
- How can ICT companies collaborate on a common freedom of expression and privacy agenda given that multiple companies' products work together as parts of one overall, interdependent network?

ii. Human rights due diligence on who ICT companies sell to, and understanding the intended use of the ICT product, service, technology or functionality.

The GNI Implementation Guidelines already have content relating to the use of human rights risk assessments to inform company strategies and approaches to freedom of expression and privacy. However, to be more relevant and useful for a wider group of ICT companies, the following questions would need to be explored in further depth:

- How can ICT companies assess the risk that customers (e.g. public sector) will use the product, service, functionality or technology being provided to violate human rights?
- What strategies can be put in place to mitigate that risk?
- What would due diligence look like at the level of the country (i.e. market entry or exit) and at the level of the customer (i.e. customers a company could choose not to sell to)?
- There are many relevant laws that already exist for customer relationships in high risk locations (e.g. export control laws), but what guidance or criteria may exist beyond this for customer engagements that may be 'legal but unethical', or which may be invasive of privacy and freedom of expression?
- How can an ICT company interpret the intended use of the ICT product, service or technology when the same functionality can be used for good or for ill? For example, the same functionality that allows remote access to a PC for maintenance and trouble shooting can have more negative applications too. What are the boundaries of responsibility for the ICT company?

iii. Many ICT companies provide consulting advice alongside the product, service or technology.

Many ICT companies not only provide hardware or software products "off the shelf" but also provide consulting advice and guidance on how to make the best use of the product or service. While it certainly can be difficult to "understand the intent" when selling a product or service "off the shelf", this position is less credible when consulting services are provided to customers alongside the product. Some questions to explore include:

- What kinds of consulting services are provided that might advise customers on how to use products for censorship or to facilitate illegitimate access to personal information?

- Can human rights guidelines be provided on the types of consulting advice that should be provided?
- What responsibility does the ICT company have if the advice about the use of their products is provided by contractors that are independent of the company – but who may have been trained by them?

iv. Responding to government demands and mandated standards.

There is a concern that companies are going to increasingly receive requests and demands from governments to modify hardware and software products in ways that will make them more freedom of expression or privacy invasive – for example, by mandating certain product functionalities or software installations. There is a great deal of content in the GNI Implementation Guidelines on how to respond to government demands, but (as described above) these cover the level of the *content or personal information*, not the level of the *functionality*. Questions include:

- How should ICT companies' respond to government demands to alter functionality or adhere to certain product standards?
- How can ICT companies collaborate with each other and with other stakeholders in response to such mandates?

2. Increasing Company Participation in the GNI

The GNI has been seeking to substantially increase company participation in its activities. These recruitment efforts started long before the GNI was launched and have continued till this day – but so far without success at securing new membership commitments. Questions from prospective member companies about GNI and its value for business are important and worth asking; participation in GNI is a meaningful commitment that we do not anticipate companies should undertake lightly. At the same time, we believe that GNI has been conscious of these legitimate concerns and responsive to them. Here we describe the five main reasons that we frequently hear from companies for not participating in the GNI, and summarize our response to those concerns.

i. "GNI's Principles and Implementation Guidelines are not relevant to our company's business"

- The core commitments in GNI are relevant to the entire ICT industry.
 - Protect and advance freedom of expression
 - Support responsible company decision making
 - Conduct human rights impact assessments
 - Collaborate with multiple stakeholders to advance human rights
- Companies that transmit information, sell network equipment, publish content, sell filtering software, or hold user data – including wired and wireless telecommunications carriers, web hosting companies, online service providers, content producers, entertainment and news media outlets, hardware and device manufacturers, and software designers – can have direct and indirect impacts on freedom of expression and privacy.
- By offering tools and a framework to support human rights due diligence and risk assessments, GNI can help all ICT companies make more responsible decisions about new products and services, potential partnerships, and market entry.

- Global telecommunications companies participated in drafting GNI's Principles and Implementation Guidelines, reflecting the interests of a broader range of companies.
- Freedom of expression and privacy are important to the entire Internet ecosystem – given the role of the private sector in building and operating this ecosystem, working together to improve respect for these rights should be part of every company's consideration of the social impacts of its operations. GNI is not only a remedial exercise for companies who have had learning experiences or challenges – it is a systematic way to improve the policy environment and help protect the well-being of individual users and customers in the ICT sector.

ii. "No other companies like ours have joined, and we don't want to make our company stand-out by joining alone"

- GNI is an opportunity to show pro-active leadership, foresight, and responsible corporate practices – something which generally is an attractive way to stand out. The ICT sector has been for some time in an era of tension between the entrepreneurial energy that leads to innovation on the one hand and society's interests in regulating technologies that are now a fundamental element of modern society on the other - tension exacerbated by the fact that social norms and their associated legal frameworks change more slowly than technologies. Every company in the ICT sector has a stake in helping to see that their own practices and their engagement in public policy navigate this era with credible guidance and with attention to preserving principles such as free expression and privacy.
- GNI provides a systematic way for companies to learn together with relevant stakeholders and socialize data about the challenges they face. Companies who are concerned about 'standing out' in terms of attracting unwanted attention should understand GNI does not have this intent.

iii. "The assessment process is too burdensome, raises legal concerns such as confidentiality, or is not suited to our company's products and services"

- The independent assessment process is critical to credibility – only through independent assessment can GNI effectively demonstrate that companies are following through on the commitments they have made and that GNI is meeting its commitment to operate in a principled, pragmatic and constructive way.
- The assessment process is primarily about learning. During the assessment process, we will learn what is working and what is not with the GNI Principles and Implementation Guidelines and make changes to our approach accordingly.
- A wide range of legal concerns (such as confidentiality requirements, trade secrets, attorney-client privilege, legal constraints) have been raised and addressed in the design of the assessment process to make it workable for companies. Google, Yahoo! and Microsoft would not be participating if the assessments had not addressed these concerns.
- Companies will be active participants in the assessment process; for example, they will select their own assessors, drawing from a pool of assessors accredited by the GNI.

iv. "GNI commitments are too burdensome for small companies to implement"

- While membership requires executive-level commitment to the principles and GNI framework, implementation of GNI commitments will vary for each company, depending on differences in size, markets, business models, products, and services.

- Assessment of a company's compliance will take the individual company's resources and business context into account. There is no "one-size fits all" approach to implementation and GNI fully anticipates that companies will find ways to implement its commitments in ways appropriate to the size, scale and scope of the participating company.

v. "Our company can implement the GNI Principles ourselves without joining GNI"

- GNI's Principles and Implementation Guidelines are in the public domain; companies can always follow the guidance GNI offers. However, a companies-only effort doesn't offer the public credibility or effectiveness of the multi-stakeholder approach. GNI is the only effort today in the ICT sector that is multi-stakeholder and that offers a third-party assessment process.
- GNI has been developed through nearly four years of intensive negotiation, collaboration, and public scrutiny and includes the commitment of some of the most prominent NGOs (Human Rights Watch, Center for Democracy & Technology, Human Rights First, Electronic Frontier Foundation, Human Rights in China, Committee to Protect Journalists, and others), academics (from Harvard, Berkeley, USC, St. Gallen, and others), and socially responsible investors (Calvert, Boston Common, F&C, Domini, and others).
- GNI enables stakeholders to come together and address global challenges and common responsibilities, and collectively create, implement, and evaluate mechanisms to protect and advance freedom of expression and privacy. An important part of how industry and civil society address these issues will be the extent to which there is a shared commitment across a broad set of stakeholders. Implementation of the principles and guidelines is important, but a shared public commitment to advance rights to freedom of expression and privacy is also an important objective, which individual implementations cannot address as effectively.

3. A shared, public, credible commitment by all companies is essential to protecting the rights to freedom of expression and privacy

It is essential that the global ICT industry and its stakeholders make a public and shared commitment to respect user rights in the face of increased threats to freedom of expression and privacy. The ICT industry is diverse, and different companies may make different decisions about entering or exiting a market based on specific circumstances such as timing, location, relationships and the nature of a particular product, service or business. There is no "one size fits all" approach to corporate responsibility, nor a single right course of action or script for all to follow. We invite all ICT companies to participate in the GNI and draw upon the guidance and insights provided by the GNI's principles and guidelines in creating a responsible approach to business decisions.

The GNI also meets Secretary of State Clinton's call for ICT companies to be able to operate in a manner that promotes respect for human rights, even in the most challenging markets. The GNI provides principles, guidelines and support to ICT companies, helping them to think through difficult choices and make decisions that protect freedom of expression and privacy for hundreds of millions of Internet users around the world.

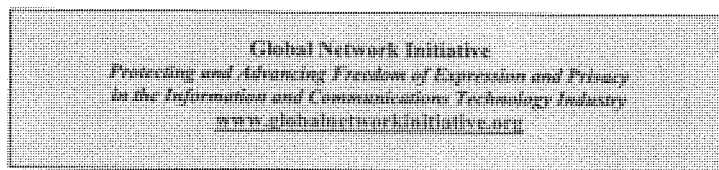
ICT companies worldwide can use the GNI's principles, guidelines and tools to assess human rights risk when entering or leaving a market or when designing and introducing new technologies, products or services. By participating in the GNI and working together with human rights groups, investors and academics, ICT companies can benefit from valuable collaboration, accountability, confidential input and collective action. These resources can help companies manage these challenges, maintain credibility and support the privacy and freedom of expression rights of their users.

The GNI's guidelines indicate that companies should:

- Establish human rights risk assessment procedures and integrate the findings into business decision-making
- Require that governments follow established domestic legal processes when they are seeking to restrict freedom of expression and privacy
- Provide users with clear, prominent and timely notice when access to specific content has been removed or blocked
- Encourage governments, international organizations and entities to call attention to the worst cases of infringement on the human rights of freedom of expression and privacy
- Utilize independent assessments of company implementation of the GNI's principles

4. Conclusion

Thank you for the opportunity to comment. GNI is committed to working with the Committee, companies, and other stakeholders to advance the respect and protection for freedom of expression and privacy around the world.



Membership Fee Structure:

Company's Annual Revenue	Annual Fee
\$0 - \$100m	\$2,000
\$100m - \$1bn	\$15,000
\$1bn - \$10bn	\$30,000
\$10bn - \$50bn	\$45,000
\$50bn +	\$60,000

Note: These fees are an 'interim membership fee'. They will be revisited during 2010 once we know how many companies have joined – and create a longer term membership fee.



August 1, 2008

Dear Senators Durbin and Coburn:

Thank you for your letter of July 21, in which you ask about the progress that we and other stakeholders have made towards finalizing a set of principles to guide Internet providers' behavior when faced with laws, regulations, and policies that conflict with global best practices on freedom of expression and privacy.

Promoting freedom of expression and privacy for users in the United States and around the world is a top priority for Google. As a company that aspires to bring the democratizing power of the Internet to individuals in every corner of every country in the world, Google helped initiate the principles process to strengthen the Internet's collective hand vis-à-vis restrictive and repressive regimes. Since the beginning of the process, our objective has been to reach agreement among a significant group of companies, investors, and non-governmental organizations on a set of clear and rigorous principles, such that restrictive governments would be unable to ignore or reject these best practices on freedom of expression and the protection of individual privacy.

As I noted in my testimony before your subcommittee on May 20, we have been working actively on the principles with all the parties involved. Since the hearing, the representatives of participating organizations reached agreement on the core components of the principles, and the materials are currently being reviewed within the individual participating organizations for approval.

The core components under review by the participating organizations are:

- Principles on Freedom of Expression and Privacy that provide direction and guidance to the information, communications, and technology industry and its stakeholders in protecting and advancing the enjoyment of freedom of expression and privacy globally.
- Implementation Guidelines that provide further details on how participating companies will put the principles into practice.
- A Governance, Accountability and Learning Framework that provides an organizational and multi-stakeholder governance structure to support the principles and a system of independent assessment to review implementation by the participating companies.

As you suggest in your letter, the principles and the group's effort to define them involve complicated issues with potentially far-reaching effects on Google's and other companies' operations. This is why the process has taken some time, and why Google is devoting significant time and effort to evaluating the principles to ensure that we can operationalize and adhere to them. We believe that it would be worse to agree to principles that will not work – which would be a cynical exercise – than to not agree to such principles at all.

*Letter to Senators Durbin and Coburn
August 1, 2008
Page 2*

Though the principles have not yet been formally agreed to by the group, 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. Consistent with those policies, we assure you that Google will not provide to the Chinese government any sensitive personal information regarding American athletes, journalists, and tourists who use the Internet while they are in China during the Olympics other than as required by United States law pursuant to the Mutual Legal Assistance Treaty or equivalent executive agreement between the U.S. and China.

With respect to censorship requests from the Chinese government, Google has established a strong track record of filtering less and providing more transparency than any other search engine in China. Our belief that we censor less than other search engines is based on our observations and on the reports of third parties. For example, a 2006 Reporters Without Frontiers report indicates that Google censors less than our search competitors in China. (Report located at http://www.rsf.org/article.php?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 conclusions. (Report located at <http://www.citizenlab.org/papers/searchmonitor.pdf>.)

In fact, the Villeneuve report states that:

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%.

We have no reason to believe that we will deviate from this strong and consistent track record.

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. And progress continues to be made. As noted in the Villeneuve report, "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."

With respect to your letter's observation that the failure to finalize the principles may suggest that congressional action may be necessary, we believe that as part of any such legislation Congress should consider the following policy recommendations, which we presented at your Subcommittee's May 20 hearing on global Internet freedom:

- **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

Letter to Senators Durbin and Coburn
August 1, 2008
Page 3

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 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. 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 Information Freedom – 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 Human Rights Committee could issue a general comment addressing relevant articles in the Covenant 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 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 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

Letter to Senators Durbin and Coburn
August 1, 2008
Page 4

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.

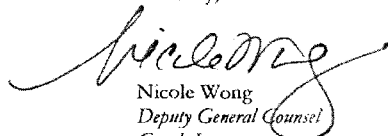
- ***Promote free expression as part of foreign aid.*** We believe that the U.S. government could use foreign aid and other programs to better promote ICCPR compliance and free expression on the Internet. For instance, the government could incorporate Internet freedom of expression into support for and assessments of good governance. In a related area, Google has already urged officials at the Millennium Challenge Corporation to incorporate Internet censorship in their criteria for measuring whether candidate countries have achieved expectations for democratic governance.

Moreover, 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.

Thank you for your attention to and leadership on the important issue of global Internet freedom. We appreciate your efforts to highlight the importance of the Internet to free expression in the United States and 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.

We look forward to serving as a resource to you and as a partner in your efforts.

Sincerely,



Nicole Wong
Deputy General Counsel
Google Inc.

United States SenateCOMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

July 21, 2008

Dr. Eric Schmidt
Chief Executive Officer
Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Dr. Schmidt:

We write to request an update on the voluntary code of conduct for internet companies that Google and other stakeholders are developing.

We discussed the code of conduct with Google Deputy General Counsel Nicole Wong during "Global Internet Freedom: Corporate Responsibility and the Rule of Law," a May 20, 2008 hearing of the U.S. Senate Subcommittee on Human Rights and the Law. As we discussed during the hearing, it is critical to the protection of fundamental human rights that a voluntary code of conduct be finalized and implemented as soon as possible.

During the hearing, Ms. Wong assured us that finalizing the code was a priority for Google, but it has been almost two months since the hearing and eighteen months since Google and other participants began to develop the code. We recognize that the code of conduct raises complicated issues with potentially far-reaching effects on your company's operations, but with every day that the code is not finalized the human rights of people across the globe are jeopardized.


We are especially concerned that the code of conduct is not yet completed because the Olympic Games will begin in China in three weeks. Without a code of conduct in place, it is more likely that Google and other American internet companies will be pressured by the Chinese government to provide sensitive personal information regarding American athletes, journalists and tourists who use the internet while they are in China during the Olympics. Moreover, in the absence of a code of conduct, it is unclear how Google and other American internet companies might respond to requests from the Chinese government and other repressive regimes to censor political or religious content.


It is also important to note that the failure to finalize a code of conduct suggests that it may be necessary for Congress to consider legislation to ensure that American companies operating in internet-restricting countries protect user privacy and freedom of expression. As Senator Durbin said during the hearing, if American internet companies are unable to regulate themselves effectively, Congress may be forced to consider doing so.

At the hearing, there was agreement that Google and other American internet companies operating in internet-restricting countries should promote free speech and not facilitate repression. A voluntary code of conduct would be one important step toward our shared goals of promoting freedom of expression and protecting the privacy of internet users around the world.

Given the importance of this issue, we would appreciate a response to this letter as soon as possible and no later than August 1, 2008. Thank you for your time and consideration.

Sincerely,


Richard J. Durbin


Tom Coburn

238

TESTIMONY OF

HUMAN RIGHTS FIRST

HEARING ON

HUMAN RIGHTS CHALLENGES FACING THE TECHNOLOGY INDUSTRY

BEFORE THE

SENATE JUDICIARY SUBCOMMITTEE ON HUMAN RIGHTS AND THE LAW

MARCH 2, 2010

Human Rights First thanks Senator Durbin and the Senate Judiciary Subcommittee on Human Rights and the Law for its ongoing leadership to examine the human rights challenges facing the technology industry. Threats to freedom of expression and privacy on the Internet and other communications technologies are gaining ground, impeding not only the freedom of individuals but also the work of civil society organizations and human rights defenders around the globe. These challenges are not limited to China and Google, and they now permeate the business environment in the technology sector. Every company in this sector with an international presence must consider the human rights impacts of its operations. Action by the Administration and the Congress is needed to ensure that U.S. policy is responsive to the challenges faced by those on the frontlines of the struggle to protect Internet freedom and that companies are being held accountable for their human rights impacts.

INTRODUCTION

New technology demands new thinking about how companies, governments and civil society groups can each work to protect freedom of expression and privacy. Each has a part to play. Secretary of State Clinton's January 21 speech marked a major turning point for promoting freedom of expression, and made clear the Obama Administration's intent to put into practice its previously stated commitment to Internet freedom - a welcome announcement. We encourage this Subcommittee to oversee these efforts, to ensure that all parts of the government concerned with this issue are coordinating their efforts behind a concrete strategy, as further discussed below. We also recommend that the Subcommittee consider several steps it can take to encourage greater transparency and attention to human rights by companies in the technology sector.

OVERSIGHT OF U.S. GOVERNMENT EFFORTS

As a starting point, the Subcommittee should help to ensure collaboration among the various agencies and offices charged with aspects of internet policy. Any U.S. policy to address threats to Internet freedom must incorporate and coordinate diplomacy, economic and security objectives. If these various efforts are not closely coordinated and aligned, there is the danger that U.S. policies in this sphere may be duplicative, or at cross purposes. It will be especially important to ensure that the various U.S. government departments and agencies transmit a consistent message to foreign governments and to the private sector on protecting Internet freedom.

The Subcommittee can also help ensure that the experiences and priorities of civil society groups and human rights defenders are taken into account as the Administration develops and implements their Internet freedom strategy.

As seen in recent events in China and Iran, as well as less publicized repression in Russia, Egypt, Belarus and elsewhere, the voices of civil society and human rights defenders are among the first to be silenced by repressive government communication technology policies. The U.S. Internet freedom strategy must focus on support for and protection of those voices. Activists from over 20 countries recently raised the importance of

protecting Internet freedom when they met with President Obama as part of the Human Rights Summit 2010 organized by Human Rights First and Freedom House.

The State Department's commitment to expand reporting on Internet freedom as part of annual country reporting on human rights will help focus attention and activities where most needed. In countries where freedom of expression is curtailed, U.S. Embassies and missions should develop plans of action for supporting the open use of communications technology by independent civil society organizations, media and human rights defenders. This would include convening regular meetings and building relationships with human rights defenders, journalists and bloggers – to show support and to remain engaged, and monitoring repressive government actions against human rights defenders. U.S. Embassies can also help bring together civil society activists, bloggers and others with technology companies operating in their countries.

Among other components of this policy as recommended by our Summit participants are: ensuring that respect for Internet freedom is a consideration in U.S. trade and investment policies, technical support and foreign assistance; reviewing U.S. export control and related policies to ensure that technology is not being denied to activists, or, conversely, being used by governments to violate the rights of activists; support for access to anti-circumvention tools; and continuing support for broadcast of news into countries where the media is heavily censored.

PRIVATE SECTOR ENGAGEMENT

The U.S. government has made clear that companies have its support in fighting repressive censorship and surveillance practices that threaten Internet freedom around the globe. But companies must do their part as well. We welcome the Subcommittee's ongoing engagement with companies to hold them accountable for the human rights impacts of their operations, and to make clear that the failure by companies to address those impacts may trigger sanctions.

Relying on individual companies to make the right decisions without mechanisms for transparency, reporting and accountability to other stakeholders simply does not go far enough to ensure respect for freedom of expression and privacy. As this Subcommittee has recognized, voluntary multistakeholder initiatives like the Global Network Initiative provide invaluable support and guidance for companies often forced to navigate difficult waters as they address the human rights impact of their operations – which involve hundreds of millions of Internet users around the world.

The Global Network Initiative is working toward a fully functioning, transparent and accountable mechanism to address human rights concerns. It has several key elements: clear standards, guidelines for implementation, and an independent assessment mechanism. It is a cost effective strategy for managing business and human rights risk, and it offers ongoing learning and expertise that no one company can provide. Human Rights First has played an active role in the development of this initiative, drawing on over 15 years' expertise in multistakeholder approaches to human rights concerns. We

hope that GNI membership will, over time, become a yardstick by which company respect for Internet freedom can be measured. We recommend that the Subcommittee continue its efforts to encourage companies to join the GNI as one way to address the human rights challenges that they face in doing business in the information sector.

We respectfully suggest that the Subcommittee consider these additional measures to encourage information technology companies to accept responsibility for the human rights impact of their business operations:

- Take the lead in development of definitions and standards on Internet freedom that are necessary to form the basis for U.S. engagement with foreign governments, companies and international institutions.
- Work with the Department of State and the GNI to support a series of convenings on privacy and surveillance issues of central concern to the technology industry, in order to develop focused recommendations for industry best practices and supportive government policies. Civil society organizations and human rights defenders in countries where Internet freedom is curtailed should be a part of these discussions.
- Request the Departments of State, Commerce and the Office of the U.S. Trade Representative to collaborate on a joint training initiative for personnel responsible for U.S. government Internet related policies and programs and other forms of industry facing engagement, in partnership with the GNI. This training should include information to assess the effectiveness of corporate policies on Internet freedom and the key components of such policies.

CONCLUSION

Human Rights First looks forward to continuing to work with Senator Durbin and the Subcommittee to ensure the development and coordination of a focused and robust U.S. policy on Internet freedom and to ensure greater private sector accountability for promoting freedom of expression and privacy in global operations.

**Written Statement for
Senate Judiciary Subcommittee on Human Rights and the Law
“Global Internet Freedom and the Rule of Law, Part II”**

March 5th, 2010

Internews Network welcomes the opportunity to provide testimony on the critical issues of internet freedom and the rule of law to the Senate Judiciary Subcommittee on Human Rights and the Law. Senator Durbin’s attention to the human rights implications of the work of technology companies and his support for the work of the Global Network Initiative, of which Internews Network is a member, are invaluable.

Internews Network and the Global Network Initiative

Internews is in a unique position among the non-governmental organizations within the GNI in that it has long-term programs in dozens of countries around the world, working with local journalists and media organizations. As the internet becomes a more critical component of the local information space in these countries, feedback from Internews’ local partners and staff touches directly on the potential human rights impacts of the activities of technology companies.

Based on this perspective, Internews would like to highlight several points:

External technical support must go beyond circumvention - As Rebecca MacKinnon¹, Ethan Zuckerman² and others have eloquently argued, there is no single “magic bullet” to combat online censorship. Even the needs for firewall circumvention itself vary tremendously from country to country and user to user and a range of solutions is needed. In addition, support for blocking-resistant hosting and other alternative publishing solutions are needed along with locally relevant education on information security broadly.

High-quality locally determined content is critically important - As Internews’ work with local media expands to include not only digital platforms but broader definitions of media creators, it is clear that no technological or other interventions from outside can replace support for the safety, skills and tools needed by local reporters (whether professional or amateur) and to efforts to create a legal, economic and social environment that enables free and informed public discussion .

Blocking or filtering of outside information is never the whole story - In all countries with significant censorship of online content from outside the country, the limiting of domestic online discourse through a variety of methods – from voluntary takedowns and self-censorship to legal or physical harassment of those who speak out – is at least equally important. No amount or type of firewall circumvention will address these problems; they require sustained legal, technical and educational activities in each country by dedicated and brave local actors.

Companies should be encouraged to expand access to their products - Internews would like to see technology companies given incentives to bring the benefits of their work to less-advantaged populations around the world. Whether through tax breaks or partnerships with non-profits or local groups, supporting the localization of software into less popular languages, affordable licensing for local media or civil society groups, and training of local technology professionals are all critical to building the capacity that will enable the growth of vibrant local information environments.

Internews has found the dialogue within the GNI to date enormously encouraging - the current company members have demonstrated not only deep commitment but creativity in addressing the human rights challenges posed by their work around the world. Other technology companies should be actively encouraged to experience the benefits that this initiative can offer them in engaging in a non-confrontational and open way with a variety of stakeholders with expertise and commitment to these issues. Internews is grateful to the committee for its attention to these issues and for the opportunity to comment.

Background

Internews Network Supports a Free and Open Internet

Internews is committed to promoting the growth of an uncensored, user-controlled and affordable internet, based on the belief that the internet plays a critical role in the flow of information that drives economic development and advances civic debate. Internews' work in supporting networked digital media, internet policy reform and technological development is grounded in the same principles that have always guided its support of independent media around the world: helping local stakeholders incorporate international standards into the work they do to inform their own citizenry.

Fundamentally, all of Internews Network's work is dedicated to increasing the availability of locally relevant news and information, allowing populations to choose for themselves what is important to their lives. In addition to providing a range of technical support to local institutions and individuals who are creating news and information, Internews also works to improve the enabling environment for independent information. What makes up this enabling environment varies tremendously from country to country.

As digital production technologies and the internet have become an integral part of the creation and delivery system for news and information, Internews' work has expanded to address these areas. Internews now trains both professional and amateur reporters in the use of digital newsgathering and works with its traditional local media partners on the challenges of the new editorial and business structures needed to build up their presence on the internet. This work also extends to projects aimed at making the internet easily accessible to the population and facilitating its growth as a platform for reliable and valuable local news and information.

Since 2000, Internews has engaged directly in the field of internet policy, working with the Center for Democracy and Technology (www.cdt.org) to create the Global Internet Policy Initiative (GIPI). GIPI brought together international expertise and in-country advocates to address such diverse issues as lobbying for changes in telephone pricing to make the use of dial-up internet more affordable, promoting legislation on electronic signatures to speed the adoption of e-commerce, and convening a group to agree on a standard for encoding different alphabets in order to promote the growth of local-language internet content.

ⁱ <http://rconversation.blogs.com/rconversation/march-2-2010-senate-testimony-on-internet-freedom.html>

ⁱⁱ <http://www.ethanzuckerman.com/blog/2010/02/22/internet-freedom-beyond-circumvention/>

Statement of

The Honorable Patrick Leahy

United States Senator
Vermont
March 2, 2010

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
Subcommittee On Human Rights And The Law,
Hearing On "Global Internet Freedom and the Rule of Law, Part II"
March 2, 2010

Today, the Subcommittee on Human Rights and the Law holds an important hearing on global Internet freedom. This important legal issue affects human rights around the globe, and it is an issue that I have worked on and championed for many years.

This decade will bring both new opportunities and new challenges for the Internet, and for the fight for human rights around the world. The Internet has become a vital tool to protect and ensure the rights and basic freedoms of Americans and the human rights of people everywhere. In today's Information Age, the Internet is perhaps the most efficient and expeditious means for spreading information about what is happening in the world, and for holding governments accountable.

One of the most pressing challenges posed by the Internet is the censorship of online information. For some time now, we have witnessed the troubling efforts of repressive regimes -- such as the governments of China, Iran and North Korea -- to censor, or in some cases eliminate, their citizens' access to information via the Internet. Most Americans are by now very familiar with the troubling reports that the government of China has hacked into the private e-mail accounts of human rights activists. We must address these serious challenges to freedom of expression head-on.

The early advances of the Internet originated in the United States, and the world rightly looks to us for leadership on matters of Internet freedom. I am very pleased that, last month, Secretary Clinton boldly reaffirmed our Nation's deep commitment to openness and freedom of expression on the Internet. The Obama administration has taken a decisive and important step.

America must also take the lead in protecting those who simply provide a platform for Internet speech from liability for the content of online speech generated by others. Our Federal laws already do this. And we must work with other nations to find the best way to promote free and open Internet speech around the globe.

Under President Obama's leadership, the United States must -- and will -- lead the way on advancing global Internet freedom. But, so too must American businesses.

Our world-class technology industry must be an integral part of the fight for global Internet freedom. During the last decade, the high tech community has developed many different kinds of anti-censorship tools to overcome firewalls and other censoring technologies. In addition, self

described "hacktivists" are also quickly developing new software to allow the citizens of China to circumvent government Internet censorship programs. I applaud these efforts and I hope that they will continue.

Today's hearing is an important opportunity to build on these successes, and to examine how best to combat Internet censorship and promote human rights in the decade ahead. Again, I thank Senator Durbin for holding this hearing, and I thank all of the witnesses for appearing before the Committee.

#####

Testimony of

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

At the hearing:

“Global Internet Freedom and the Rule of Law, Part II”

Senate Judiciary Committee
Subcommittee on Human Rights and the Law

March 2, 2010

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

My name is Rebecca MacKinnon. I am currently a visiting fellow at Princeton University’s Center for Technology Policy. Earlier in my career I worked as a journalist for CNN in China, living in Beijing for more than nine years. For the past six years while based at several different academic institutions I have researched Chinese Internet censorship alongside global censorship trends, examining in particular how the private sector assists government efforts to silence or manipulate citizen speech. In 2006 I became involved in discussions between members of industry, human rights groups, investors, and academics which eventually led to the formation in 2008 of the Global Network Initiative, the non-governmental multi-stakeholder initiative that aims to help Internet and telecommunications companies uphold the principles of free expression and privacy around the world. I am also co-founder of an international bloggers’ network called Global Voices Online, which is now five years old and has an active community of contributors from more than 100 countries. Several of our community members have been jailed or exiled because of their online activities, and many more have been threatened. My testimony today is informed by my experience as a journalist who has lived under and reported on authoritarian controls firsthand; as a researcher of Internet censorship; as a practitioner of new media; and as an advocate for free expression and human rights on the Internet.

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

- 1 -

Authoritarianism is adapting to the Internet

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

In the four years since the late Rep. Lantos' famous February 2006 hearing where Google, Yahoo, Microsoft and Cisco first defended their business practices in China, the number of Internet users on the planet has almost doubled. Yet according to the latest "Freedom of the World" study released by Freedom House, the overall level of freedom in the world declined in 2009 for the fourth consecutive year.¹ Ironically, many of the countries with the most serious declines in freedom are also experiencing rapid growth in Internet and mobile usage. Take China, for example. The number of Chinese Internet users quadrupled in the past four years. It is true that the Internet has enabled people to expose corruption, bring justice to innocent victims of official malfeasance, and even change some laws and regulations, in ways that were not possible in the past. But this has not led to the overall strengthening of rule of law, greater independence of the courts from the Communist Party, or greater protection of civil liberties by the system as a whole. According to the Dui Hua Foundation, in 2008 arrests and indictments on charges of "endangering state security" - the most common charge used in cases of political, religious, or ethnic dissent - more than doubled for the second time in three years, and the trend is expected to continue when figures come out for 2009.² China is pioneering new, flexible but effective methods to control and manipulate online speech and suppress citizen dissent - not controlling everybody and everything one hundred percent, but squashing or isolating certain types of Internet speech effectively enough that they can prevent reform movements from succeeding, or in some cases even from emerging.

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

¹ *Freedom in the World 2010*, by Freedom House, February 2010, at:

<http://www.freedomhouse.org/template.cfm?page=505>

² "Chinese State Security Arrests, Indictments Doubled in 2008," *Dui Hua Human Rights Journal*, March 25, 2009, at: <http://www.duihua.org/hrjournal/2009/03/chinese-state-security-arrests.html>

use Internet and mobile technologies to their own advantage. Iran is one of China's most eager students, as the Ahmadinejad regime finds ways to counter the Green Movement's use of technology. The Iranian government recently set up an official cyber defense command under the Islamic Revolutionary Guards Corps to fight "cyber crime" – with "crime" defined broadly to include criticism of the Ahmadinejad regime.³ Last month Iran's chief of police warned protestors against using e-mail, text messaging and social networks to organize demonstrations. "The new technologies," he said, "allow us to identify conspirators and those who are violating the law without having to control all people individually."⁴

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

The expanding toolbox of Internet controls

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

- **Filtering or "blocking:"** This is the original and best understood form of Internet censorship. Internet users on a particular network are blocked from accessing specific websites. The technical term for this kind of censorship is "filtering." Some congressional proceedings and legislation have also referred to this kind of censorship as "Internet jamming." Filtering can range in scope from a home network, a school network, university network, corporate network, the entire service of a particular commercial Internet Service Provider (ISP), or all Internet connections within a specific country. It is called "filtering" because a network administrator uses special software or hardware to block access to specified web pages by banning access to certain designated domain names, Internet addresses, or any page containing specified keywords or phrases. A wide range of commercial filtering products – including SmartFilter now sold by McAfee – are

³ "In Run-Up to Islamic Revolution Day 2010, Iranian Regime Steps Up Oversight, Censorship on Media, Citizens," *The Middle East Media Research Institute*, February 5, 2010 at: <http://www.memri.org/report/cn/0/0/0/0/0/3956.htm>

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

developed and marketed here in the United States by U.S. companies for use by parents, schools, government departments, businesses, and anybody else who wants to control how their networks are used. All Internet routers – including those manufactured by the U.S. company Cisco Systems – come with the ability to filter because it is necessary for basic cyber-security and blocking universally reviled content like child pornography. However, the same technology can just as easily be used to block political content. According to the Open Net Initiative, an academic consortium that has been following global Internet filtering since 2002, more than forty countries now practice Internet filtering to some extent at the national level. As this Committee is well aware, China's Internet filtering system – known to many as “the Great Firewall of China” – is the most sophisticated and extensive in the world. Researchers believe Iran to have developed the world's second-most comprehensive system of filtering. But filtering is widely deployed on the national level in Asia, the Middle East, and increasingly though more narrowly in Europe.⁵

- **Deletion and takedown of content by Internet companies:** Filtering is the primary means of censoring content over which an authority has no jurisdiction. When it comes to websites and Internet services over which a government does have legal jurisdiction – usually because at least some of the company's operations and computer servers are located in-country – why merely block or filter content when you can delete it from the Internet entirely? The technical means for deleting content, or preventing its publication or transmission in the first place, vary depending on the country and situation. The legal mechanism, however, is essentially the same everywhere. In Anglo-European legal systems we call it “intermediary liability.” The Chinese government calls it “self-discipline,” but it amounts to the same thing, and it is precisely the legal mechanism through which Google's Chinese search engine, Google.cn, was required to censor its search results.⁶ All Internet companies operating within Chinese jurisdiction – domestic or foreign – are held liable for everything appearing on their search engines, blogging platforms, and social networking services. They are also legally responsible for everything their users discuss or organize through chat clients and messaging services. In this way, much of the censorship and surveillance work in China is delegated and outsourced by the government to the private sector – who, if they fail to censor and monitor their users to the government's satisfaction, will lose their business license and be forced to shut down. It is also the mechanism through which China-based companies must monitor and censor the conversations of more than fifty million

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

⁶ See *Race To the Bottom: Corporate Complicity in Chinese Internet Censorship* by Human Rights Watch (August 2006), at <http://www.hrw.org/reports/2006/china0806/>. Also “Search Monitor Project: Toward a Measure of Transparency,” by Nart Villeneuve, Citizen Lab Occasional Paper, No.1, University of Toronto (June 2008) at <http://www.citizenlab.org/papers/searchmonitor.pdf>

Chinese bloggers. Politically sensitive conversations are deleted or blocked from being published at all. Bloggers who get too influential in the wrong ways can have their accounts shut down and their entire blogs erased. That work is done primarily not by “Internet police” but by employees of Internet companies.⁷

- **Cyber-attacks:** The sophisticated, military-grade cyber-attacks launched against Google were targeted specifically at the GMail accounts of human rights activists who are either from China or work on China-related issues. This serves as an important reminder that governments and corporations are not the only victims of cyber-warfare and cyber-espionage. Human rights activists, whistleblowers and dissidents around the world, most of whom lack training and resources to protect themselves, have over the past few years been victim of increasingly aggressive cyber attacks.⁸ The effect in some cases is either to bring down dissident websites at critical political moments or for frequent short periods of time, putting a great strain on the site’s operators just to keep the site running and preventing them from doing their main work. Targets range from Chinese human rights defenders to an independent Russian newspaper website, to Burmese dissidents, to Mauritanian opponents of military dictatorship.⁹ On December 17, 2009, the home page of Twitter – which was instrumental in spreading word about protests in Iran – was hacked by a group calling itself the “Iranian cyber army.” Twitter was back up after a couple of hours. An Iranian Green Movement website Mowjcamp.com was attacked on the same day but – lacking the same resources and clout as Twitter and hampered by U.S. laws that forbid American web hosting companies from doing business directly with Iranians – remained offline for more than six weeks.¹⁰

In other cases cyber attacks compromise activists’ internal computer networks and e-mail accounts to the point that it becomes too risky to use the Internet at all for certain kinds of organizing and communications, because the dissidents don’t feel confident that any of their digital communications are secure.

⁷ For more details see “China’s Censorship 2.0: How companies censor bloggers,” by Rebecca MacKinnon, *First Monday* (February 2006) at:

<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089>

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

⁹ “Chinese human rights sites hit by DDoS attack,” by Owen Fletcher, *ComputerWorld*, January 26, 2010, at: <http://www.computerworld.in/articles/chinese-human-rights-sites-hit-ddos-attack>; “Russia’s Novaya Gazeta Web site hacked, paralyzed” by David Nowak, Associated Press, February 1, 2010 at: <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/01/AR2010020102424.html>; “Web Sites Back Online, but Fears of Further Attacks Remain,” by Min Lwin, *Irawaddy*, September 22, 2008, at:

http://www.irawaddy.org/article.php?art_id=14294; “Dictators Prefer Botnets,” Strategy Page, November 18, 2008, at: <http://www.strategypage.com/htm/htiw/articles/20081118.aspx>

¹⁰ “Yahoo!, Moniker: why is Mowjcamp.com still offline 6 weeks after hack attack?” by Ethan Zuckerman, *My Heart’s in Accra*, February 1, 2010, at: <http://www.ethanzuckerman.com/blog/2010/02/01/yahoo-moniker-why-is-mowjcamp-com-still-offline-6-weeks-after-hack-attack/>

Likewise, journalists who report on human rights problems and academics whose research includes human rights issues have also found themselves under aggressive attack in places like China, exposing their sources and making it much more risky to work on politically sensitive topics. Like the activists, these groups are equally unprepared and unequipped to deal with such attacks.¹¹

- **Compliance with political “law enforcement”:** In countries whose governments define “crime” broadly to include political dissent, companies with in-country operations and user data stored locally can easily find themselves complicit in the surveillance and jailing of political dissidents. This committee is of course very familiar with the most notorious example of law enforcement compliance gone wrong: between 2002 and 2004 Yahoo’s local China-based staff handed over to the Chinese police e-mail account information of journalist Shi Tao, activist Wang Xiaoning, and at least two others engaged in political dissent.¹² There are other examples. Skype partnered with a Chinese company to provide a localized version of its service, then found itself being used by Chinese authorities to track and log politically sensitive chat sessions by users inside China.¹³ This happened because Skype delegated law enforcement compliance to its local Chinese partner without sufficient attention to how the compliance was being carried out.
- **Device-level and local controls:** In late spring of 2009 the Chinese Ministry of Industry and Information Technology (MIIT) mandated that by July 1st of that year all computers sold in China must be pre-installed with a specific software product called “Green Dam – Youth Escort.”¹⁴ While the purpose of “Green Dam” was ostensibly for child protection, researchers inside and outside of China quickly uncovered the fact that it not only censored additional political and religious content, it also logged user activity and sent this information back to a central computer server belonging to the software developer’s company.¹⁵ The

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

¹² See “Shi Tao, Yahoo!, and the lessons for corporate social responsibility,” working paper presented at presented December 2007 at the International Conference on Information Technology and Social Responsibility, Chinese University, Hong Kong, at: <http://reconversation.blogs.com/YahooShiTaoLessons.pdf>

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

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

¹⁵ *China's Green Dam: The Implications of Government Control Encroaching on the Home PC*, Open Net Initiative bulletin (June, 2009) at: <http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc>; *Analysis of the Green Dam Censorware System*, by Scott Wolchok, Randy Yao, and J. Alex Halderman, Computer Science and Engineering Division, The University of Michigan, June 11, 2009, at: <http://www.cse.umich.edu/%7Fjhalderm/pub/gd/>.

software had other problems that made it easy for U.S. industry to oppose: It contained serious programming flaws which increased the user's vulnerability to cyber-attack. It also violated the intellectual property rights of a U.S. company's filtering product. Faced with uniform opposition from the U.S. computer industry and strong protests from the U.S. government, the MIIT backed down on the eve of its deadline, making the installation of Green Dam voluntary instead of mandatory.¹⁶ The defeat of Green Dam, however, did not diminish other efforts to control and track Internet users at more localized levels inside the national "Great Firewall" system – for instance at the level of a school, university, or apartment block as well as at the level of a city-wide Internet Service Provider (ISP). It was reported in September last year that local governments were mandating the use of censoring and surveillance products with names like "Blue Shield" and "Huadun." The function and purpose of these products appeared similar to Green Dam, though they had the benefit of involving neither the end user nor foreign companies.¹⁷ The implementation of these systems has received little attention outside of China.

Recommendations

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

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

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

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

¹⁷ "China Clamps Down on Internet Ahead of 60th Anniversary," by Owen Fletcher, IDG News Service, September 25, 2009 at: http://www.pcworld.com/article/172627/china_clamps_down_on_internet_ahead_of_60th_anniversary.html ; and "China: Blue Dam activated," by Oiwan Lam, *Global Voices Advocacy*, September 13, 2009 at: <http://advocacy.globalvoicesonline.org/2009/09/13/china-blue-dam-activated/>

important step of joining the Global Network Initiative (GNI), a code of conduct for free expression and privacy in the ICT sector. The GNI can help companies uphold a shared commitment to the values of free expression and privacy while recognizing that no market is without political difficulties or ethical dilemmas.

Just as companies have a social responsibility not to pollute our air and water or exploit twelve-year-olds, companies have a responsibility not to collaborate with the suppression of peaceful speech. The GNI's philosophy is grounded in the belief that people in all markets can benefit from Internet and mobile technologies. In most cases companies can contribute to economic prosperity and individual empowerment by being engaged in countries whose governments practice some of the Internet controls I have described above – as long as they are aware of the human rights implications of their business and technical decisions. It is fundamentally reasonable to expect all companies in the ICT sector to include human rights risk assessments in their decisions about market entry and product development, just as they and other companies consider environmental risks and labor concerns.

With a multi-stakeholder membership including human rights groups, socially responsible investors and academics like myself, GNI's goal is to help companies do the right thing while bringing expanded Internet communications and mobile access to the people who stand to benefit most from these technologies. All GNI members are participating in this process because we believe in the transformative importance of the ICT sector and want innovative businesses to be successful and competitive. We are working with companies in good faith. I personally believe that the GNI member companies are managed by people who want both to do well and to do good, but who recognize that they face difficult problems, and that they could use support and advice in order to avoid mistakes. As an academic researcher and free speech advocate, my goal in working with GNI member companies is to help them foresee and avoid mistakes long before they happen. When mistakes do happen, companies should be held appropriately accountable in ways that can help the entire industry learn from these mistakes and do a better job of avoiding them in the future.

GNI's principles are supported by implementation guidelines and an accountability framework that can be adapted to a range of business models, including hardware companies and Internet service providers, if these companies choose to engage with the GNI. We look forward to working with them so that it will be possible for them to join in the near future. While GNI is presently most relevant to Yahoo, Google and Microsoft because those were the three companies that launched the initiative, it is also clear that the thirty companies contacted by you, Mr. Chairman, share varying degrees of human rights risk, even as their business models, technologies, and geographies vary widely. They have an obligation to at least consider joining the GNI and if they choose not to, to find other appropriate policy and operational responses to address the inescapable human rights implications of their products or services.

- **Legislative measures:** Congress has a range of legislative tools at its disposal. Some should be implemented as soon as possible, while others may take more time and consideration in order to ensure that they are proportional, appropriate, and effective.
 - ***Legal support for victims:*** Companies will have a further disincentive to collaborate with repressive surveillance and censorship if victims or corporate collaboration in human rights abuses can more easily sue them in a U.S. court of law.
 - ***Incentives for socially responsible innovation:*** Established companies as well as entrepreneurial new startups should be encouraged, perhaps through tax breaks and other incentives, to develop technologies and features that enhance users' ability to evade censorship and surveillance, as well as to help users better understand what personal information is being stored, how it is used, and who has access to it.
 - ***Upgrade export controls:*** Existing export control laws require updating in order to remain consistent with their intent in the Internet age, in two ways:
 - Halt denial of service to human rights activists: The United States has several laws that bar the sale of specific kinds of software to, or forbid business transactions with, individuals and groups from specified countries. These laws do not take into account new Internet developments, and as a consequence have resulted in denial of website hosting and other services to dissident groups from repressive nations. U.S. laws – exacerbated by corporate lawyers' over-cautious interpretation of them – have recently prevented U.S. web-hosting companies from providing services to opposition groups based in Iran, Syria and Zimbabwe. They should be upgraded as soon as possible so that American Internet businesses can welcome rather than turn away some of the world's most vulnerable and politically isolated groups.¹⁸
 - Make collaboration with repression more difficult: Recognizing that no connectivity at all is even worse than censored connectivity, and also recognizing that many information communications technologies have "dual use" capabilities that are used for legitimate security and law enforcement as well as repression, it should nonetheless be made more difficult for U.S. companies to provide censorship and surveillance capabilities to

¹⁸ "Not Smart Enough: How America's "Smart" Sanctions Harm the World's Digital Activists," by Mary Joyce, Andreas Jungherr and Daniel Schultz, DigiActive Policy Memo for the Commission on Security and Cooperation in Europe, October 22, 2009, at: <http://www.digiaactive.org/2009/10/22/digiaactive-policy-memo-to-the-us-helsinki-commission/>

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

- ***Technical support for free expression:*** People in repressive regimes require support in a broad range tactics and technologies – along with the training and education in their use – to reflect the growing sophistication with which governments are stifling and silencing peaceful speech. In addition to helping people around the world to circumvent Internet blocking, we need to help people fight cyber-attacks, counter-act content removal by companies, fight deployment of device-level spyware and censorware, and educate each other quickly about new forms of technical control as new methods and technologies emerge.
- Circumvention technologies: Congress deserves great praise for its allocation of funds over the past few years to support the development of tools and technologies that help Internet users in repressive regimes circumvent Internet filtering. Support for a healthy range of circumvention tools – in a manner that fosters competition, innovation, accountability, and user choice – is important and must continue. The problem is that circumvention tools only address Internet filtering: they don't address other methods of control that repressive regimes now use to censor Internet content and silence dissent. Thus, an effective Internet freedom strategy cannot focus on circumvention alone.
- Anonymity and security: In my interactions with journalists, human rights activists, civil liberties lawyers, bloggers, and academics in authoritarian countries around the world, I have found that a shockingly large number are uninformed about how to evade online surveillance, how to secure their e-mail, how to detect and eliminate spyware on their computers, and how to guard against even the most elementary cyber-attacks. Local-language, culturally appropriate technologies, accompanied by robust education and training, is desperately needed. The recent cyber-attacks against Chinese GMail users only highlights the urgency.
- Preservation and re-distribution of deleted content: In the course of my research about the Chinese Internet, I have noticed that quite a lot of people around Chinese blogosphere and in chatrooms make a regular habit of immediately downloading interesting articles, pictures, and videos which they think those materials could get deleted or taken offline. They then re-post these materials in a variety of places, and relay them to friends through social networks and e-mail lists. This is done in an ad-hoc way. Thus, it is often difficult for people to locate and spread this material. The United States should support the creation of searchable, accessible, and

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

- Distributed “opposition research”: After the Chinese government mandated the nation-wide installation of the “Green Dam” censorware last year, loosely organized “opposition research” networks sprang into action. A group of Chinese computer programmers and bloggers collectively wrote a report exposing Green Dam’s political and religious censorship, along with many of its security flaws. They posted the document at Wikileaks.¹⁹ This information was then used by domestic and foreign opponents of Green Dam in a successful campaign to reverse the government’s mandate. Another anonymous group of Chinese netizens have collected a list of companies and organizations – domestic and foreign – who have helped build China’s Internet censorship system.²⁰ Opposition research has also helped to expose the Tunisian government’s use of cutting-edge “deep packet inspection” techniques for censorship and surveillance. In 2008 Global Voices Advocacy Director Sami Ben Gharbia – a Tunisian exile – conducted tests that demonstrated DPI being used in Tunisia to block certain emails, or even alter certain contents of emails like attachments.²¹ If people in repressive regimes had better mechanisms through which to collect and share information about how their governments are stifling free expression, it would be easier for activists around the world to help each other develop effective technologies and tactics to fight back.
- ***Other legislative measures***: Further legal steps may be necessary to ensure adequate respect for human rights by companies that fail to take voluntary action. It is important, however, that any law be flexible enough to accommodate the rapidly-changing nature of information communications technology, as well as the complex and highly diverse

¹⁹ “A technical analysis of the Chinese “Green Dam Youth Escort” censorship software,” posted June 2009 on Wikileaks.org at:

http://wikileaks.org/wiki/A_technical_analysis_of_the_Chinese_%27Green_Dam_Youth-Escort%27_censorship_software (At time of writing the page cannot be reached due to bandwidth and funding problems at Wikileaks.org)

²⁰ “GFW Engineering Team Name List,” posted to Google Documents in January 2010 at:

<http://docs.google.com/View?docid=0Ac8NBXfKcGvqZGR0am1yeGRfMWhyZDljcWY4>

²¹ “Silencing online speech in Tunisia,” by Sami Ben Gharbia, *Global Voices Advocacy*, August 20, 2008, at: <http://advocacy.globalvoicesonline.org/2008/08/20/silencing-online-speech-in-tunisia/>

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

- **Censorship as barrier to trade:** A number of prominent experts in trade law in North America and Europe have argued that Internet censorship should be considered a barrier to trade under the World Trade Organization. In November the European think tank ECIPE concluded that WTO member states are “legally obliged to permit an unrestricted supply of cross-border Internet services.”²² The United States Trade Representative should be encouraged to pursue cases against China and other countries that block their citizens from accessing the online services of U.S. Internet companies.
- **Continued executive branch leadership.** Secretary of State Clinton’s landmark speech on Internet freedom made it clear that this is a core American value. She has placed the United States squarely in a leadership position by identifying a range of threats to Internet freedom, as well as the range of tools and policies that can be brought to bear. In reviving the Global Internet Freedom Task Force (GIFT), the Administration now has a mechanism to coordinate between government and industry to ensure that U.S. companies play a constructive role around the world. GIFT will also need to tackle the challenging job of coordinating between all the different U.S. government agencies whose work touches upon the Internet in various ways. If we are serious about promoting global Internet freedom, it is important that U.S. foreign policy, trade, commerce, and national security all be consistent in advancing Internet freedom.

Conclusion

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

²² “Protectionism Online: Internet Censorship and International Trade Law,” by Brian Hindley and Hosuk Lee-Makiyama, ECIPE Working Paper No. 12/2009, at: <http://www.ecipe.org/protectionism-online-internet-censorship-and-international-trade-law/PDF>

Testimony of Omid Memarian
Hearing on "Global Internet Freedom and the Rule of Law, Part II"
U.S. Senate Judiciary Subcommittee on Human Rights and the Law

March 2, 2010

Mr. Chairman, members of the Subcommittee;

I welcome this opportunity to speak on the important matter of Internet freedom. I hope our efforts might help people around the world, including in my home country of Iran, to have more access to information via the Internet and the other means of communication enjoyed around the world today.

My name is Omid Memarian. I am a journalist and senior researcher for the International Campaign for Human Rights in Iran, an independent nonprofit that monitors Iran's compliance with international human rights standards.

For many in this room, access to information via the Internet might seem a natural part of their daily routine. But millions of people around the world fight to enjoy such access, including the people of Iran. In 2004, I was arrested by the Iranian security forces and held in a secret prison and in a solitary confinement. Then I was taken to Evin prison, where hundreds of political prisoners are being kept since the June 12th presidential elections. During my time in solitary confinement, I was beaten and physically and psychologically tortured, and told that I should stop posting my writings on my blog and stop working as a journalist. There was no actual crime in my case; I was arrested and abused for using the Internet to share information. Since then, hundreds of journalists, bloggers and civil society activists who have used the Internet to study and learn, and to spread their ideas and messages, have been detained. Just last year, the blogger Omid Mirsayyafi died in detention.

When I moved to the United States in 2005, I learned that my website had been shut down. But don't get me wrong, it was not the Iranian government who shut down my website, it was the domain and host provider in the US that did it. In an email, the company mentioned the restriction on any transaction with Iranian companies. I learned later that many other pro-democracy and pro-human rights websites had to change their domain on account of those restrictions, and get dot.ir domains, which can be easily monitored by the Iranian authorities.

The June 12th elections and massive reactions to the reported results evoked a violent crackdown. Those who used YouTube videos, social networking websites and chat rooms to send out the people's narrative of the events, rather than the government's narrative have come under particular pressure. While their efforts have been not only extremely influential, but also breathtaking, inspiring and informative, they have been very costly for those who fight for freedom of speech and free access to the Internet.

Access to information in general and to the Internet in particular is an inseparable part of human rights. Protecting it is the shared responsibility of our time. Since the election,

I've worked with human rights organizations and news agencies to document the post election violence in Iran. I've learned that if it had not been for the government's extensive crackdown on the Internet and on the other means of communication, more people would have known what was going on, and the government would not have been able to pursue its bloody repression. We have learned in school that "information is power". In some countries, information and spreading the truth among the people means saving lives and alleviating the suffering of those who are in pain. That's why I, and many of my fellow citizens, who are aggressively trying to stop the tragic human rights violations in Iran by gathering and spreading information about current events, believe that providing Internet access for the Iranian people, and other people in the world in similar conditions, is not a political, but a moral act. There is a direct, and positive connection between free access to Internet-information, and the quality of people's lives.

The Internet continues to be a powerful medium for propagating political opinions, information on corruption, injustices and human rights violations, and other information that is essential to holding governments accountable to their citizens, as well as facilitating exchanges of perspectives. And that trend has been accelerating. Iranian bloggers are amongst the top 10 most active in the world, even though thousands of blogs and political websites -- and even Google-- have been filtered in Iran. The fact that some governments prevent free access to the Internet for their people is not all about politics. It is also an effort to control cultures by preventing their people from experiencing new ideas and values that connect them to the rest of the world and let them develop their capacities as human beings. Such governments, including the Iranian government, prevent their people from engaging with the international community and the global economy and culture, just because they have chosen the path of marginalization and irresponsibility.

Iran is among very few countries in the Middle East where, if free and fair elections were held tomorrow, radicals and fundamentalists would not come to power. Iran's vibrant civil society, educated population and thriving younger generation have been pushed back by repression.

I believe that countries that have faith in the freedom of speech, and freedom of access to the Internet as a mean to achieve that, have a crucial role to reach out and help citizens of states that reject those internationally guaranteed human rights.

When I decided to participate in this hearing, I talked to many of my friends-- bloggers, journalists and those who have difficulties to even send a simple email or chat on Yahoo messenger. Almost all of them believe that any kind of support to give Iranians more access to the Internet is supporting human rights and democracy in the country, supporting security in the Persian Gulf region, and most importantly saving the lives of many people who are threatened by restrictions on information that allow the Iranian government to operate behind closed doors as it violates their basic rights.

Almost all of them believe that it's a form of moral support. It should not be seen or used as a means to pursue hidden political purposes, but as promoting human rights as defined by international standards. Providing Internet access for Iranians should not be seen as a part of a possible regime change plan in Iran, because it is up to the Iranian people to

decide what to do with their freedom. The Iranian people, with all the characteristics that I mentioned above, are capable of making decisions for their future. But supporting efforts to provide them free access to information and Internet gives them the possibility to enjoy rights to information and communication that belong to them, as they belong to all people.

Some of you in this room might think that Iran's nuclear program is the most urgent issue that the United States and other members of the international community are facing today. But this is wrong. I can assure you that you can easily reach a deal with the Iranian government over its nuclear development program. But how legitimate, or trustworthy, could such an agreement be, when the government kills innocent protesters on the streets and tortures people inside the prisons? Providing free access to Internet for the Iranian people and human rights defenders, journalists and activists, sheds light on the governments' notorious actions and allows the citizens to hold them accountable for their policies and practices.

This is not a local issue. It concerns a country stuck between other countries that either suffer from radicalism or that export terrorists to the rest of the world, a country between two major sources of conflict in the region, Iraq and Afghanistan. That's why such support is directly related to the security of the region and the world in a long run.

We should not forget that if it were not for the Internet, we would have the same picture of the Iranian government that we had 9 months ago. And if it were not for the limited access to Internet that exists, God knows how many more people would have been killed or tortured inside prisons in Iran.

As a journalist and human rights defender, I would like to stress the importance of applying standards in a balanced—not political—way. Not only Iran, but numerous other countries, violate the right to access the Internet, and the United States should support compliance across the board. Otherwise, the charge of holding double standards will stick.

With that in mind, I would like to make four main points in my testimony this morning in relation to global Internet freedom:

Modifying the U.S. sanctions on Iran

Certain sanctions or interpretations of the sanctions have seriously damaged the ability of Iranians to access the Internet and need to be modified.

1) Software download is blocked to IPs from Iran: Many of major companies such as Google and Microsoft block downloads to people in Iran in fear of sanctions. For example, Google Talk or Google Chrome, one of the safest web browsers, is not available for download to Iranian users. This policy is only harming ordinary Iranian users, since the Iranian government can already download such software through its proxies in Europe and Dubai. All mass market software which is useful for publishing, communications, and education should be exempted from the sanctions.

2) Online advertising is not allowed for Persian websites: Many companies such as Google or Facebook do not include Persian (Farsi) as a supported language for online advertising websites or allow targeting users with such a language. This is problematic when activists want to use such advertising tools to reach out to Iranians in Iran. It also prevents many of the human rights activist websites from making small amounts of money on advertising that can help them to pay for their server costs. There is no money transaction involved between Iran and U.S. This is about allowing advertising to be shown on websites in Persian that are based outside of Iran.

3) Concerning allowing people in Iran to pay for domain purchase and related issues, many of the domains belonging to Iranian human rights activists were stolen by Iranian government-sponsored hackers because such activists have difficulties registering such domains under their names and have to do this through proxies. As a result there is no way to verify their location or identity when their web domains are stolen. Just in the past few months, a few hundred domains registered on Godaddy have been stolen by the Iranian government and there is no way to get them back because the original owners were not allowed to buy those domains legally on Godaddy in the first place.

4) Funding is needed to allow hiring a limited number of web developers in Iran. Many of the small activist groups need to hire developers to build their websites. The number of web developers with a command of the Persian language outside of Iran is very few. These groups need to be allowed to hire web developers in Iran. The amount of payments could be capped to \$10000 per year to make sure such a solution is not abused for other purposes.

5) Online access and advertising should be exempted from the current sanction regime via a categorical order. Without a categorical order, such a problem can not be solved. The reason is that the Iranian market is very small and many of the US-based Internet companies prefer to stay away from it instead of spending tens of thousands dollars on legal fees to apply for an export license.

6) European companies who still sell surveillance or censorship technology to the Iranian government need to be exposed and face sanctions. A number of large European companies have provided Iranian government with technologies to monitor SMS and communications between Iranians. Without the pressure from the U.S. government, it is unlikely that the European Union will take actions against them.

With regard to how Iranians can be supported in terms of Internet access and security, and how some of the online activism can be supported financially, I advocate for the following:

Internet access

1) Giving VPN accounts to the activists and journalists in Iran: VPN provides the best security and functionality compared to any other solution. VPN accounts would need to be bought from different VPN providers and distributed to the activists through different online websites. Each major human rights or pro-democracy website would be given

between 100-500 VPN accounts. They would distribute them to trusted activists in Iran they know.

2) Purchasing Skype credits for activists in Iran: Using Skype credits, activists in Iran can make secure international calls. Skype's encryption is one of the best among all the voice services.

3) Anti-jamming for satellite broadcasts: The Iranian government sends jamming signals to commercial satellites. Many of the commercial carriers are reluctant to broadcast independent or reform-oriented Iranian TV content because their satellite can be blinded by the Iranian government. Commercial satellites can be jammed because the upload and download signal is the same and the upload signal is a fixed frequency. However, military satellites are built to resist such jamming. For Iranian broadcasts, the US government could dedicate a specific satellite, which is hardened against jamming using technologies similar to military satellites.

4) Provide Iranians with free satellite Internet: The technology for Internet access is not cheap but considering the importance of Internet access in Iran, it is worth investing on this issue. There are technologies for one-way delivery of content or two-way interactive Internet access. Providing such services free of charge to the Iranian people can go a long way in breaking the monopoly of the Iranian government on the dissemination of information in Iran.

5) Email security: Unfortunately, no secure free email provider exists. Yahoo is particularly insecure, while Gmail provides more security but is still vulnerable to key loggers. For activists, there is a need for an email service to have security as high as PayPal accounts or bank accounts. For example, the login process should be resistant against keyloggers. This can be achieved by showing images or other techniques.

6) PC security: One idea is to provide the activists with free security software and anti-virus software.

Collaborating with the human rights community

Finally, private companies and initiatives can provide resources to support the development of technology designed to combat internet censorship including those technologies that surpass filters. There are a number of professionals and companies that are focused on developing software that provide such technologies for Iranian users that could be supported.

Thank you again for this opportunity to speak on this important subject.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
<http://www.microsoft.com/>



August 1, 2008

Honorable Richard J. Durbin
309 Hart Senate Office Building
Washington, DC 20510

Honorable Tom Coburn
172 Russell Senate Office Building
Washington, DC 20510

Dear Senators Durbin and Coburn:

Thank you very much for your letter of 21 July 2008 to Steve Ballmer. Steve shared your letter with me and has asked me to reply on his behalf.

Microsoft welcomes this opportunity to provide you with an update on the multi-stakeholder discussions referenced in your letter. As you know, the goal of these discussions is to develop broadly accepted principles that companies will observe when responding to government actions that threaten to restrict freedom of expression or compromise fundamental privacy protections.

We are pleased to report that representatives of the diverse group of human rights organizations, policy groups, companies, socially responsible investors, and academics working on these principles have reached agreement in principle on the core components of a planned ICT ("Information, Communications, and Technology") Initiative. The agreement in principle is now being reviewed by each participating entity for final approval, and for a decision whether to participate in (or, as may be appropriate for some entities, simply to endorse) the Initiative.

Later this year, once these approvals and participation decisions are made, the Initiative's members, plans, and details will be formally announced. At this time, however, we can provide you with some information about the core components of the Initiative, which are as follows:

Principles on Freedom of Expression and Privacy that provide direction and guidance to the ICT industry and other stakeholders on protecting and advancing rights to freedom of expression and privacy globally. The Principles describe key commitments in the following areas: Freedom of Expression; Privacy; Responsible Company Decision Making; Multi-Stakeholder Collaboration; and Governance, Accountability & Transparency.

Microsoft Corporation is an equal opportunity employer.

Page 2
August 1, 2008

Implementation Guidelines that provide further detail on how participating companies will put the Principles into practice. The Implementation Guidelines describe a set of actions which, when followed by a company, would constitute compliance with the Principles, and thereby provide companies with concrete guidance on how to implement the Principles.

A Governance, Accountability and Learning Framework founded on the notion that an organizational and multi-stakeholder governance structure is required to support the Principles and that participating companies should be held accountable for adhering to the Principles through a system of independent assessment.

Companies participating in the Initiative will put the Principles into practice throughout their operations over time, and there will be milestones in terms of reporting along the way. Additionally, the companies and other participants will be working collectively to consider options for public policy engagement, to strengthen government respect for freedom of expression, and to carry out the independent assessments that are part of the accountability process.

We realize there is still much work to be done, but we are optimistic that we are laying the foundation for a meaningful, integrated, and sustainable approach that will address root causes and help the ICT sector protect and advance fundamental rights to freedom of expression and privacy in the ICT sector.

Over the next few months, the Initiative will be finalizing organizational steps, allowing time for participants to obtain internal approvals and plan for the significant organizational commitments represented by the Initiative. We anticipate a more detailed public announcement to launch the Initiative sometime this fall.

Microsoft is pleased to be working with human rights advocacy groups, academics, and investors to move these principles forward and to address these issues in a practical and operational way. This continues to be a constructive and positive engagement. The diversity of membership within the Initiative is indicative of the broad-based commitment by all parties to protect and advance human rights. It has also given us the valuable opportunity to work with and learn from many different perspectives that nonetheless share a common goal.

The Initiative is open to new participants - both companies and non-companies - that would like to join or indicate their support for the Initiative prior to its launch.

Page 3
August 1, 2008

In addition, an important part of the Initiative's work will be to socialize its principles with companies and organizations around the globe, with the goal that the Principles and other core elements will take root as an international standard, and generate further understanding of the goals, intentions, and the international orientation that informs the Initiative's work.

Microsoft believes in freedom for users to connect to the people and information that is important to them. Even while we continue to work to move the Initiative forward, we will adhere to current company policies that aim to help protect our users's privacy and freedom of expression when faced with government demands that impact those rights.

This includes our existing company policy with respect to government demands to remove access to blog content posted to Microsoft's Windows Live Spaces service, and our existing policy on how we respond to law enforcement requests for information about our subscribers.

Specifically, existing company policy provides that Microsoft will block access to Windows Live Spaces content only where we receive a legally binding notice from a government indicating that the material violates local laws, or if the content violates our terms of use. We remove access to content only in the country issuing the order, to the extent technically possible, and we let users in that country know why content was blocked, notifying them that access has been limited due to a government restriction.

Additionally, we respond to government requests for subscriber information only pursuant to authorized law enforcement requests which follow applicable legal process. Where that data is stored in the United States, Microsoft will comply with applicable U.S. laws protecting online privacy, including the requirements of the Electronic Communications Privacy Act. Where appropriate, we direct foreign governments seeking access to such data to follow international agreements that require established government-to-government procedures. Microsoft also applies internal risk assessment procedures aimed at protecting user privacy.


We agree that Internet communications companies can and should play a valuable role in advancing the achievement of human rights, including freedom of expression. It is important to Microsoft that the Internet be fostered and protected as a worldwide tool for reliable information and communications, personal expression, innovation, and economic development.

Page 4
August 1, 2008

As we have done to date, Microsoft is happy to respond to additional questions, and we remain open to meeting with you and your staff to discuss these issues further.

Thank you again for your letter and please let us know if you have any additional questions.

Best regards,

A handwritten signature in black ink, appearing to read "Pamela S. Passman". The signature is fluid and cursive, with the first name "Pamela" being more prominent than the last name "Passman".

Pamela S. Passman
Corporate Vice President, Global Corporate Affairs

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

July 21, 2008

Steven A. Ballmer
Chief Executive Officer
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Dear Mr. Ballmer:

We write to request an update on the voluntary code of conduct for internet companies that Microsoft and other stakeholders are developing.

The code of conduct was discussed during "Global Internet Freedom: Corporate Responsibility and the Rule of Law," a May 20, 2008 hearing of the U.S. Senate Subcommittee on Human Rights and the Law. As we discussed during the hearing, it is critical to the protection of fundamental human rights that a voluntary code of conduct be finalized and implemented as soon as possible.

It has been almost two months since the hearing and eighteen months since Microsoft and other participants began to develop the code. We recognize that the code of conduct raises complicated issues with potentially far-reaching effects on your company's operations, but with every day that the code is not finalized the human rights of people across the globe are jeopardized.

We are especially concerned that the code of conduct is not yet completed because the Olympic Games will begin in China in three weeks. Without a code of conduct in place, it is more likely that Microsoft and other American internet companies will be pressured by the Chinese government to provide sensitive personal information regarding American athletes, journalists and tourists who use the internet while they are in China during the Olympics. Moreover, in the absence of a code of conduct, it is unclear how Microsoft and other American internet companies might respond to requests from the Chinese government and other repressive regimes to censor political or religious content.

It is also important to note that the failure to finalize a code of conduct suggests that it may be necessary for Congress to consider legislation to ensure that American companies operating in internet-restricting countries protect user privacy and freedom of expression. As Senator Durbin said during the hearing, if American internet companies are unable to regulate themselves effectively, Congress may be forced to consider doing so.

At the hearing, there was agreement that Microsoft and other American internet companies operating in internet-restricting countries should promote free speech and not

facilitate repression. A voluntary code of conduct would be one important step toward our shared goals of promoting freedom of expression and protecting the privacy of internet users around the world.

Given the importance of this issue, we would appreciate a response to this letter as soon as possible and no later than August 1, 2008. Thank you for your time and consideration.

Sincerely,



Richard J. Durbin



Tom Coburn

Testimony of Michael H. Posner
Assistant Secretary of State for Democracy, Human Rights and Labor
Senate Judiciary Human Rights and the Law Subcommittee
“Global Internet Freedom and the Rule of Law, Part II”
March 2, 2010

Chairman Durbin, Senator Coburn and Members of the Committee, thank you for holding this important hearing. I am pleased to be with you today to discuss U.S. efforts to promote and protect Internet freedom.

This past year we have seen more and more people around the globe gaining greater access to more information through the Internet, cell phones and other forms of connection technologies. From Iran to China, from Egypt to Colombia, activists, journalists and ordinary citizens are using digital technologies to spread and access information in real time. Simultaneously, too many governments are spending more time, more money and more attention to implement regulatory and technical mechanisms that are intended to curtail freedom of expression and the free flow of information.¹

As the Internet and other connection technologies evolve and the number of users multiplies, the State Department is committed to defending freedom of expression and the free flow of information on this new terrain of the 21st century. In her recent speech at the Newseum, Secretary Clinton emphasized that the defense of a free, open and interconnected Internet is in our national and global interests and is important for commerce, for diplomatic and political relations, and for building sustainable democratic societies.

The Department is committed to implementing the Secretary’s vision for Internet freedom. In partnership with Members of Congress, with increased resources and through a variety of tactics, we are working to promote Internet freedom as a key component of our foreign policy.

Within the Department, the Under Secretary for Democracy and Global Affairs Maria Otero and Under Secretary for Economic, Energy and Agricultural Affairs Robert Hormats lead our efforts on Internet freedom. Since 2006, the Under Secretaries have chaired an Internet freedom taskforce, which was officially re-launched last week as the NetFreedom Taskforce. The Taskforce serves as a policy-coordinating body within the Department and includes participation from the regional bureaus, public affairs and the Office of the Legal Adviser. The taskforce’s leadership by the Under Secretaries for

¹ One need only look to the headlines to see this point illustrated: “Cyberactivists Get Help from YouTube, U.S. to Thwart Repression” by Indira A.R. Lakshmanan, Bloomberg, February 22, 2010; “Clinton: Google China Case Raises Serious Concerns” by Andrew Quinn, ABC News, January 12, 2010; “Vietnam Facebook fans fear government blackout” by Ben Stocking, The Associated Press, November 17, 2009; and “State Dept. to Twitter: Iran too important, site fix can wait” by Monica Guzman, The Big Blog, Seattle Post-Intelligencer, June 16, 2009.

Economics and for Global Affairs reflects the Department's commitment to aligning our principles with our business interests.

The NetFreedom Taskforce operates according to three core principles: advancing Internet freedom through expanded access to the Internet; monitoring Internet freedom; and responding to threats to Internet freedom.

Advancing

The Department funds programs that support unrestricted access to online content through technology, training and increased access for marginalized groups. Beginning in 2008, the Bureau of Democracy, Human Rights and Labor (DRL) has implemented \$15 million in programming in support of Internet freedom, and we will soon award more than \$5 million in additional funding.

The goal of DRL's Internet freedom programming is simple: unfettered, safe access to information and communications for more people in more places.

To achieve this objective, we support the development of new tools that enable individuals to exercise their right to freedom of expression by circumventing politically motivated censorship and technological barriers to secure person-to-person communications. We fund groups around the world to make sure these tools get to the people who need them, in their local languages. And we provide training in how to access and use the Internet safely. In our latest request for proposals, we focused on access to information on mobile devices and cyber-security for NGOs and digital activists, which we have identified as emerging trends.

But DRL is not the only government entity focusing on this issue; others, such as USAID and the Office of the Middle East Partnership Initiative (MEPI), also fund innovative programs that promote freedom of expression and the free flow of information on the Internet and other connection technologies:

- Both USAID, through its democracy and governance programs, and DRL, through its human rights and democracy programs, train journalists, civil society activists, and political parties in the use of new Internet and other digital technologies to disseminate messages, empower individual voices, and encourage transparency. USAID and DRL media programs support citizen journalists and work to promote a legal framework that allows for freedom of expression and independence in both print and Internet media.
- USAID recently launched a public-private partnership with the Knight Foundation to implement the MATADOR (Media Assistance utilizing Technological Advancements and Direct Online Response) program, which trains and supports civil society groups and NGOs in the use of new media technologies that enhance communication and coordination efforts.

- This year, MEPI plans to support a series of pilot projects to expand the new media capabilities of civil society and enhance online learning opportunities in the Middle East and North Africa.

In addition to programming, the Department advances Internet freedom through official human rights dialogues and economic dialogues, and in multilateral organizations. For example, we will make Internet freedom an important agenda item in the upcoming Communications and Information Policy Dialogue and the Human Rights Dialogue with China. I have raised the issue in informal meetings with government counterparts, as have Ambassador Phil Verveer and Under Secretaries Hormats and Otero. We are deploying our diplomatic resources not only to speak out when threats to Internet freedom arise, but also to build alliances to promote Internet freedom.

Monitoring and Analyzing

The second of our core principles is monitoring. Monitoring threats to Internet freedom informs our policymaking and programming decisions. Since 2006, we have reported on Internet freedom in our annual human rights reports, which will be released later this month. In 2010, we are undertaking a review of the human rights reporting process and will improve our Internet freedom reporting to be more detailed and dynamic. We will also work with experts in the field of counter-censorship to make the human rights reports more accessible to people with limited or restricted Internet access. And we are increasing the capacity of embassy officers to monitor and respond to threats to Internet freedom by developing a training course at the Foreign Service Institute specifically on the topic of Internet freedom.

From 2007 to 2009, the Department has funded spatial analysis of blogospheres in order to better understand relationships among interests within particular language groups.

Through the NetFreedom Taskforce, we have established a working-level group on Internet freedom that will staff the Under Secretaries on these issues. It will meet regularly to coordinate and implement policy, activities and programming on the topic. We are using technology to improve coordination and information-sharing among this group so that we are better able to quickly identify emerging threats to Internet freedom.

Responding

The third and final principle guiding our Internet freedom efforts is responding to threats to Internet freedom. As threats arise, we will work diligently to ensure that all State and government-wide assets provide a coordinated and effective response, including diplomatic, technical and public diplomacy strategies. We engage vigorously with foreign governments when bloggers or digital activists have come under attack or when content or services are blocked. For example, when a popular social networking site was blocked in Vietnam late last year, we raised the issue with government officials in Washington and Hanoi. When bloggers, in countries such as China and Egypt, are

threatened and persecuted for what they post online, we speak out on their behalf. And when countries adopt repressive laws that restrict Internet access, we speak out against those efforts, as we have in Kazakhstan and Belarus, and pursue bilateral and multilateral initiatives to address the problems.

We also engage with technology firms and civil society organizations on the issue of censorship. As referenced in the Secretary's speech at the Newseum, Under Secretaries Hormats and Otero will convene a meeting of technology executives this Thursday at the State Department to discuss Internet freedom. I will be part of that meeting, as will Ambassador Verveer. Both Ambassador Verveer and I have been meeting with NGOs and companies since the Secretary's speech and will continue to seek their input as we develop our policy in response to new threats and emerging trends. The NetFreedom Taskforce will convene a meeting this summer with external stakeholders to address emerging threats and opportunities to promote Internet freedom.

The Department is supportive of voluntary action by industry to improve Internet freedom, such as through the Global Network Initiative (GNI), a multi-stakeholder initiative that includes companies, NGOs, investors and academics. We share your enthusiasm for action by companies on this issue in a multi-stakeholder setting, with a clear set of principles, guidelines for implementing those principles, and a means for verifying compliance.

Finally, Mr. Chairman, our partnership with and support from those in Congress, like you and this Committee, are important and vital to this issue. It will be very helpful to have both the Executive and Legislative branches signaling the importance of Internet freedom and freedom of expression. I want to thank you again for convening this hearing, for the very important and timely work of this Committee, and for your leadership. I am keen to continue the conversation, consult with the Committee on the issue of Internet freedom and to work together in the future to advance Internet freedom. I am happy to answer your questions.

REPORTERS WITHOUT BORDERS FOR PRESS FREEDOM	Washington DC, March 2nd, 2010 WRITTEN STATEMENT
--	---

"GLOBAL INTERNET FREEDOM AND THE RULE OF LAW, PART II"

WHAT U.S. COMPANIES SHOULD BE DOING TO INSURE THAT THEY ARE NOT COMPLICIT IN
HUMAN RIGHTS VIOLATIONS RELATING TO INTERNET FREEDOM.

Each year, Reporters Without Borders publishes an "Internet enemies" list, naming about twenty countries where Internet censorship is an obstacle to individual freedoms, either by surveilling the network, harassing the bloggers and filtering websites. Ten days from now, the new list will be published. Out of the 12 Internet Enemies the organization listed last year, at least one U.S. Internet company was involved in the Internet industry in many of them. The challenge for these firms is to keep their human rights standards while doing business in these repressive countries. They have to fight the local law, which asks them to display the data of their clients, if the government requests it, no matter how (a phone call could be enough). This is exactly what happened back in 2004 with the sadly famous Shi Tao case, involving Yahoo ! in the Chinese censorship.

In April 2004, the Chinese journalist **Shi Tao** used his Yahoo! email account to send a message to a U.S.-based pro-democracy website. In his email, he summarized a government order directing media organizations in China to downplay the upcoming 15th anniversary of the 1989 crackdown on pro-democracy activists. Police arrested him in November 2004, charging him with "illegally providing state secrets to foreign entities." Authorities used email account holder information supplied by Yahoo! to convict Shi Tao in April

Reporters Without Borders USA - 1500 K street NW # 600 - Washington, DC
20005

P : 202 256 5613 - Clothilde Le Coz - E : clc@rsf.org

[25 YEARS]

2005 and sentence him to 10 years in prison. It is believed that four other dissidents have been convicted because of Yahoo's involvement in China.

U.S Internet firms and their implication is Internet censorship

Google, Yahoo ! and Microsoft are the three Internet Giants worldwide. And they are American. Google is still censoring its search engine in China although it is reconsidering its position there. It will also be submitted to restrictions in Sri Lanka, as the government stated at the beginning of this year. Blogspot, its blog platform, is submitted to restricted rules in Vietnam. A government notice, Circular n°7, came into force on 20 January 2009, which is designed to control blogs and their content. It is now illegal for a blogger to post articles under another identity. Blogs can only carry strictly personal information (Article 1) and it is banned to "put out press articles, literary works or other publications banned by the press law" (Article 2). Moreover, every six months, at the request of the authorities, hosts must make a report on the activities of their customers including the number of blogs they run and their statistics as well as details of blogs that violate rules established by the host (Article 6). Microsoft is harshly censoring the results of its search engine Bing in China too. According to *The New York Times*, "Microsoft apparently doesn't want to pursue the Google solution of having separate sites - one that produces generally legitimate results (google.com) and another within China that blatantly censors (google.cn). Instead, Bing figured it would have one site and just censor all the results in simplified Chinese characters."

In order to fight the local law forcing the U.S firms to censor online free speech, two initiatives were born in 2006: The Global Online Freedom Act (GOFA) and the Global Network Initiative (GNI).

Why Reporters Without Borders thinks the GOFA is the best way for U.S firms to insure Internet Freedom

Reporters Without Borders USA - 1500 K street NW # 600 - Washington, DC
20005

P : 202 256 5613 - Clothilde Le Coz - E : clc@rsf.org

[~~25 YEARS~~]

Reporters Without Borders believe that, as of today, the best option to prevent IT companies from being forced to collaborate with the Web-censors in repressive countries remains to provide a legal framework for companies willing to resist governments' requests that violate the international free speech standards, as the Global Online Freedom Act, introduced by Representative Chris Smith does for American IT firms. Reporters Without Borders has supported the Global Online Freedom Act (GOFA) since its birth. Introduced by Representative Chris Smith (R-NJ) in February 2006, it would protect American IT companies from being forced to collaborate with repressive regimes. The Act would prevent repressive governments - those that punish dissidents and human rights activists who exercise their right to online free expression - from accessing personal data through US companies.

The bill would ban companies from locating the servers containing this data and from providing information that identifies users, except in cases in which the law is being legitimately applied, to be decided by the US justice department. The US companies would also have to act transparently and transmit information about the type of censorship they apply to an interagency-staffed Office of Global Internet Freedom, which would have the job of defining US government policy for the promotion of the free flow of online information and monitoring violations. A feasibility study of technologies and equipment's export control would also be made. The bill also promotes the idea of a voluntary code of conduct to be established for companies working in countries with repressive regimes.

The GOFA is a draft law being studied in the United States and in a different version within the EU. It was proposed in the House of Representatives by Republican Deputy Christopher Smith in a new version on 6 May. Inspired by the Foreign Corrupt Practices Act, it aims to prevent US companies from "cooperating with repressive governments in transforming the Internet into a tool of censorship and surveillance." It also aims to ensure that the US government fulfils its responsibility "to promote freedom of expression on the Internet" and "restore public confidence in the integrity of US businesses."

Reporters Without Borders USA - 1500 K street NW # 600 - Washington, DC
20005

P : 202 256 5613 - Clothilde Le Coz - E : clc@rsf.org

[25 YEARS]

The European version of GOFA was put before the European Parliament on 17 July 2008 by Dutch member, Jules Maaten of the Alliance of Liberals and Democrats for Europe (ALDE), and was inspired by the US model. It urges European companies to assume their "responsibility to uphold the principles of the Universal Declaration of Human Rights" and requires them to locate their servers outside repressive countries.

The Global Network Initiative is a coalition that includes ICT companies, civil society organizations (including human rights and press freedom groups), socially responsible investors and academics. Three US firms are so far involved : Google Inc, Yahoo ! Inc and Microsoft Corp. The goal is for the membership to be global and to be from across the internet and telecommunications industries. The foundational documents reflect over two years of extensive engagement and negotiation by the participants and were collaboratively drafted by the multi-stakeholder group over an 18-month period, from January 2007 through June 2008. The work of key academic institutions, consultations with other stakeholders, and the experiences of other voluntary human rights initiatives influenced the drafting. Reporters Without Borders took part in the negotiation but did not sign the Global Principles on Freedom of Expression and Privacy. However, the organization recognizes it as a first step towards ICT companies' recognition of the importance of free expression while operating in Internet-restricting countries.

Under these principles, another Shi Tao case is still possible.

Recommendations

Reporters Without Borders

- urges the House of representative to pass the Global Online Freedom Act and take a clear stance on it
- encourages the US Internet Firms to follow Google's lead and reconsider their involvement in China.
- Asks the US government to ensure that the sponsorship for online circumvention tools is effective.

Reporters Without Borders USA - 1500 K street NW # 600 - Washington, DC
20005

P : 202 256 5613 - Clothilde Le Coz - E : clc@rsf.org

[25 YEARS]

- Asks the Congress to launch an Internet Freedom Caucus as soon as possible

Reporters Without Borders USA - 1500 K street NW # 600 - Washington, DC
20005

P : 202 256 5613 - Clothilde Le Coz - E : clc@rsf.org

[~~25 YEARS~~]



United States Department of State

Washington, D.C. 20520

DEC 15 2009

Dear Mr. Chairman:

The enclosed report is being provided consistent with Section 1606 of the Iran-Iraq Arms Non-Proliferation Act of 1992 (P.L. 102-484) (the "Act"). The Under Secretary of State has determined that the issuance of a license for a proposed export to Iran is "essential to the national interest of the United States." The attached report provides a specific and detailed rationale for this determination. The waiver authority under Section 1606 of the Act will not be exercised until at least 15 days after this report is transmitted to the Congress.

The Department of State is recommending that the Department of Treasury's Office of Foreign Assets Control (OFAC) issue a general license that would authorize downloads of free mass market software by companies such as Microsoft and Google to Iran necessary for the exchange of personal communications and/or sharing of information over the internet such as instant messaging, chat and email, and social networking. This software is necessary to foster and support the free flow of information to individual Iranian citizens and is therefore essential to the national interest of the United States.

Please do not hesitate to contact us if we can be of further assistance.

Sincerely,

A handwritten signature in black ink, appearing to read "Richard R. Verma".

Richard R. Verma
Assistant Secretary
Legislative Affairs

The Honorable
Carl Levin, Chairman,
Committee on Armed Services,
United States Senate.

Report under the Iran-Iraq Arms Non-Proliferation Act of 1992

This report is being provided consistent with Section 1606 of the Iran-Iraq Arms Non-Proliferation Act of 1992 (P.L. 102-484) (the "Act"). Section 1603 of the Act applies with respect to Iran certain sanctions specified in paragraphs (1) through (4) of Section 586G(a) of the Iraq Sanctions Act of 1990 (P.L. 101-513) (the "ISA"). This includes the requirement under Section 586G(a)(3) of the ISA to use the authorities of Section 6 of the Export Administration Act of 1979 ("EAA") to prohibit the export to Iran of any goods or technology listed pursuant to Section 6 of the EAA or Section 5(c)(1) of the EAA on the control list provided for in Section 4(b) of the EAA, unless such export is pursuant to a contract in effect before the effective date of the Act (October 23, 1992).

Pursuant to Section 1606 of the Act, the President may waive the requirement to impose a sanction described in Section 1603 of the Act by determining that it is essential to the national interest of the United States to exercise such waiver authority. On September 27, 1994, the President delegated his authorities under the Act to the Secretary of State. Subsequently, on January 12, 2007, the Secretary of State delegated these authorities to the Under Secretary for Arms Control and International Security (DA 293-1).

Personal internet-based communications are a vital tool for change in Iran as recent events have demonstrated. However, U.S. sanctions on Iran are having an unintended chilling effect on the ability of companies such as Microsoft and Google to continue providing essential communications tools to ordinary Iranians. This waiver will authorize free downloads to Iran of certain nominally dual-use software (because of low-level encryption elements) classified as mass market software by the Department of Commerce and essential for the exchange of personal communications and/or sharing of information over the internet. The waiver will enable Treasury's Office of Foreign Assets Control to issue a broader general license covering these downloads and related services. This general license will be comparable to exemptions which already exist for the exchange of direct mail and phone calls. The new general license will specifically exclude from its authorization the direct or indirect exportation of services or software with knowledge or reason to know that such services or software are intended for the Government of Iran.

The Under Secretary has determined that it is essential to the national interest of the United States to exercise the authority of Section 1606 of the Act not to impose the sanction described in Section 1603 of the Act and Section 586(a)(3) of the ISA and to permit the issuance of a general license for this kind of software.

The Washington Post

What Hillary Clinton, Google can do about censorship in China

Advertisement

By Caylan Ford
Wednesday, January 20, 2010; 2:14 PM

Google announced last week that it is no longer willing to censor its Chinese searches and may soon be closing its offices in China, and Secretary of State Hillary Clinton will be rolling out a new policy initiative concerning internet freedom on Thursday.

But if the State Department and internet giants really want to promote free access to the Internet worldwide, the most effective thing they could do is to support the Global Internet Freedom Consortium (GIF).

GIF is a small outlet run by a group of Chinese-American computer scientists. Over the last ten years, they have developed a suite of censorship-circumvention software that allows users to safely evade internet firewalls and surveillance. They have no offices or funding. Their scientists work day jobs and pay for their operations out of their own pockets. Yet in spite of their obvious limitation, they are responsible for approximately 90 percent of all anti-censorship internet traffic in China and Iran.

When protests erupted in Burma in 2007 and its military junta moved to violently suppress demonstrations, it was GIF software that activists used to relay images, video and information to the rest of the world. When riots erupted in Tibet in 2008, GIF's traffic from the region rose by 300 percent. And when Iranians took to the streets to demonstrate against suspected election fraud in 2009, over 1 million Iranians per day were using GIF software to communicate with the outside world. Without GIF, there could have been no "Twitter revolution."

But GIF servers, which can currently support only 1.5 million unique users per day, nearly crashed in the aftermath of the Iranian election. With a small amount of funding or with private donations of server bandwidth, GIF could increase its capacity to support 50 million users.

Of course, even with more resources, anti-censorship technology can still be thwarted. Governments can simply restrict access to the Internet altogether, as Iran did last summer, or as Chinese authorities did in Xinjiang province recently. China's "green dam youth escort," an unwieldy pre-installed software that censors politically sensitive information in individual computers, could also significantly undercut the efficacy of circumvention tools.

But in a country such as China, whose economy is now deeply tied to the Web, shutting down the Internet or crippling computers with "green dam"-like software is enormously unpopular and expensive. For every dollar spent on censorship-circumvention, repressive regimes must sacrifice hundreds or thousands of dollars to counter it.

Even so, GIF hasn't received a penny of funding from either the U.S. government or private corporations. That could be because the software engineers behind GIF are adherents of Falun Gong, a Buddhist spiritual discipline that is banned and brutally repressed in China. Since 1999, hundreds of thousands of Falun Gong believers have been sent to forced labor camps and tortured, and the Communist Party has blocked information about Falun Gong on the Internet and in the media. GIF

engineers began their work largely so that their compatriots in China could access and share information about the persecuted spiritual practice. In a Washington Post article last week, an unnamed U.S. official was quoted as saying that "the Chinese would go ballistic" if GIF received government funding.

But any truly effective measures to promote Internet freedom will irk dictatorships. If the U.S. government wishes to promote internet freedom, it must be prepared to cope with the blow-back.

The United States already devotes considerable resources to promoting democratization, press freedom and human rights initiatives every year. For a small fraction of that budget, America can provide free access to information to tens of millions of people.

Caylan Ford is a graduate student in international affairs at the George Washington University. She is a volunteer editor and analyst with the Falun Dafa Information Center, though the views expressed in this article are hers alone.

[View all comments](#) that have been posted about this article.

Post a Comment

[View all comments](#) that have been posted about this article.

You must be logged in to leave a comment. [Login](#) | [Register](#)

Submit

Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will take steps to block users who violate any of our posting standards, terms of use or privacy policies or any other policies governing this site. Please review the [full rules](#) governing commentaries and discussions. You are fully responsible for the content that you post.

Sponsored Links

Acai Berry WARNING!

Exposed Acai Berry: Health Reporter's Shocking Discovery
www.ConsumerProductsDaily.com

Earn an MBA - No GMAT!

Earn Your MBA From a Top Ranked University without the GMAT. Learn How Now!
USNewsUniversityDirectory.com/MBA

Smoking Can Be Healthy?

Read the Report on New Cigarettes That Don't Kill. Smoke Anywhere Now!
www.HealthReportsToday.com

[Buy a link here](#)

© 2010 Washingtonpost.Newsweek Interactive

Testimony of Daniel J. Weitzner
Associate Administrator for Policy Analysis and Development
National Telecommunications and Information Administration
United States Department of Commerce

Before the
Subcommittee on Human Rights and the Law
Committee on the Judiciary
United States Senate

Human Rights Challenges Facing the Technology Industry

March 2, 2010

I. Introduction.

Chairman Durbin, Ranking Member Coburn, and Members of the Subcommittee, thank you for this invitation to testify on behalf of the Department of Commerce and the National Telecommunications and Information Administration (NTIA) on certain global challenges facing the Internet industry. As an advocate of economic growth, innovation, and exports, the Department of Commerce's goal is to support a global, open Internet as a platform for the free flow of information goods and services. In the Internet marketplace, as with all other major areas of economic activity, the Department of Commerce is committed to our role as partner with U.S. companies, large and small, as they grapple with the challenges associated with operating in countries that do not share the commitment of the United States to openness, transparency and the free flow of goods and services. The Internet is a globally interconnected network, meaning that even the smallest U.S. Internet start-up can be reached by any Internet user globally, and that, conversely, the U.S. economy can become the target of foreign laws, rules, and actions even where it has no foreign presence.

Since its commercial launch, the Internet has proven to be not only an extraordinary platform for information in sharing but also a primary medium for the efficient, free flow of goods and services. Over the last 15 years, it has been a driver of growth in virtually all sectors of the U.S. economy. This growth generates jobs, and it sustains our international competitiveness in an increasingly interconnected global economy.

Between 1999 and 2007, the U.S. saw an increase in business-to-consumer Internet commerce by over 500 percent. When business-to-business transactions are taken into account, online commerce in 2007 accounted for over three trillion dollars in business revenue for U.S. companies. It is critical that U.S.-based online commercial interests be able to operate under transparent rules and on a level playing field.

Today, I would like to summarize what the Department of Commerce has observed as some of the challenges facing U.S. industry, discuss the importance of transparency in the Internet, and update you on current Department of Commerce activities to support the worldwide commercial robustness of the Internet.

II. Challenges Faced By U.S. Companies.

U.S. companies face a number of challenges offering Internet-based goods and services around the world that threaten the continued growth of the Internet as a platform for global commerce. There are three specific challenges faced by U.S. companies that the Department of Commerce believes are particularly troubling.

First, an increasing number of foreign countries are imposing forms of censorship on the Internet. As a result, U.S. companies are often pressured to block or filter Internet content or

communications absent any evidence of illegality and based on rules that can be unclear, not committed to writing, or are enacted without adequate due process or transparency. U.S. companies are placed in the untenable situation of trying to divine what content they should filter in order to satisfy the arbitrary and not transparent requirements imposed by certain foreign nations. Often faced with threats of personal criminal or civil liability for their employees, U.S. companies have been forced to either over-block content to the detriment of their customers and their own business interests, or under-block (from the perspective of the foreign government) thereby risking loss of liberty or the ability to do business there. These restrictions impede the flow of legitimate products and services by placing unreasonable and vague compliance burdens on U.S. businesses.

Second. U.S. companies are often subjected to excessive and sometimes repressive surveillance demands from foreign nations. Foreign governments may require Internet Service Providers (ISPs) or other Internet businesses to provide assistance in electronic surveillance without due process or adequate judicial supervision. For example, some governments require that all Internet traffic be routed through one government-controlled access provider or facility, so that they can use monitoring software to track activities of individual users. Further, some governments require U.S. businesses operating within their borders to conduct surveillance or surrender stored information about users. Forcing U.S. Internet companies to comply with secretive government surveillance demands also undermines trusted consumer relationships between U.S. companies and their customers, both in the U.S. and worldwide.

Third. U.S. companies risk being the victims of hacking attempts sponsored by overseas criminals, foreign agents or loose-knit groups of the same. These threats place at risk the

integrity of data held in trust by U.S. companies on behalf of their employees and customers. It puts at risk valuable commercial information including intellectual property, customer data, internal proprietary information, and confidential business plans. And, in certain circumstances, these hacks can become the pretext for forced compliance with government imposed technical standards that are overly prescriptive. This last practice puts all network services at risk and unfairly disadvantages U.S. companies that tend to rely on global, voluntary consensus-based standards. Furthermore, in this era of globally-integrated services and cloud computing platforms, cybersecurity threats in one country have implications far beyond the borders of that country, putting proprietary information, customer data and operational readiness at risk of an entire global enterprise. These risks can constitute a price so high that U.S. companies may avoid doing business altogether in such environments.

III. Greater Transparency is key to the operation of the global, open Internet.

Secretive, aggressive treatment of Internet users and online service providers such as those described here threaten one of the most important aspects of the Internet's *modus operandi* – transparency. Transparency has been a vital feature of the Internet's technical design, its cooperative administrative systems, and many of the business arrangements that have led to its breath-taking, global success. Open technical standards have enabled rapid innovation, high quality technical design, and global interoperability of underlying network services and the applications that run on those networks. Threats to global technical transparency for the purpose of sheltering domestic activities and vendors in a single country are barriers to global online commerce and pose a threat to leading U.S. technology companies

– as well as other companies that operate in countries dedicated to openness and due process of law. Just as important as technical transparency is openness and clarity of laws that apply to Internet-based commercial and non-commercial activity.

Transparency is an indispensable foundation of the Internet's global reach. Without technical and operational transparency, the ability of the Internet to function as a single, global platform will be gradually undermined. While recent security threats have directed our attention to vulnerabilities in the Internet's infrastructure, we must not lose sight of the extraordinary engineering achievements that enables to citizens and business of the world to communicate through a common platform.

In looking ahead towards any new U.S. government involvement in this arena, the Department of Commerce will continue its tradition of working with stakeholders in the U.S. and abroad to develop government-industry-civil society partnerships that encourage all businesses to operate with transparency, wherever located. From a public policy perspective, we fully understand that safeguarding the Internet's openness – and even fostering greater openness – is a complex task. For the most part, Internet governance historically has done well with private sector leadership. And despite recent challenges, we are hopeful that industry will continue to foster concrete, evolutionary changes in the way businesses respond to overly intrusive government restrictions. As evidenced by the creation of the Global Network Initiative (GNI) several years ago, industry, civil society organizations, investors and academics all have vital leadership roles to play in helping businesses develop credible, accountable systems. We will know that these systems are succeeding when they enable us to assess both company and country compliance with openness and internationally recognized human rights

laws and standards. The Department of Commerce and NTIA have been heartened by GNI's ongoing efforts to develop and refine a voluntary code of conduct for technology companies that do business in challenging governmental environments. We continue to monitor their progress. At the same time, we believe we have an ongoing obligation to assess whether and, if so where, greater government support to the private sector might be warranted.

IV. Commerce Department Initiatives to Address the Broad Challenges of Internet Policy.

Ensuring that the Internet is open for innovation and social progress both domestically and globally is a vital task for the nation and, therefore, for the Department of Commerce. To that end, our Department assembled months ago an Intra-agency Internet Policy Task Force whose mission is to identify leading public policy and operational challenges in the Internet environment. Along with this public policy assessment, we are exploring steps to assist companies to operate responsibly and competitively even in markets that lack the level of openness, due process, and respect for internationally recognized human rights laws and standards that we believe to be vital to the Internet.

The Department of Commerce is drawing upon our expertise across many bureaus, including international communications policy, trade, intellectual property, business advocacy, and corporate responsibility, to develop comprehensive responses to these issues. Our work began with the Administration's efforts in developing an Internet privacy and cyber-security framework that meets the needs of the 21st Century information economy. Thus far, the Task Force has convened listening sessions with officials from major U.S. corporations and technology companies across the country. In these sessions, Commerce representatives

solicited private sector input on how to enable innovation in information services, while protecting individual privacy rights and security both in the United States and around the world. We have now added to that agenda consideration of trade barriers such as the concerns identified in this hearing, along with online copyright enforcement and the future of multi-stakeholder governance. In the coming months, the Task Force will be releasing a Notice of Inquiry in the Federal Register to reach out further to American industry and civil society groups. It is anticipated, that based on this feedback, the Task Force will make formal recommendations to the Secretary of Commerce on public policy positions and operational initiatives to enhance the free flow of information goods and services on the Internet.

V. Conclusion.

Today, in certain parts of the world, U.S. companies face increasing pressure to comply with policies and official practices in ways that conflict – or at least create substantial tension – with internationally recognized human rights laws and standards. This impedes the free flow of information goods and services on the Internet and has a negative impact on global economic growth and innovation. The Department of Commerce believes that greater transparency is essential to preserving an open Internet, which, in turn, is a key priority of the Obama Administration. Transparency shines a positive light on effective national policy and regulatory practices and is equally important as a tool to draw attention to impediments to the free flow of information goods and services. We look forward to continuing our work with our colleagues at the State Department, other federal agencies, and Congress to develop the most effective

policy framework to enable U.S. companies all citizens of the world to have access to an unfettered flow of information goods and services online.



**Testimony of Nicole Wong, Vice President and Deputy General Counsel,
Google Inc.
Before the U.S. Senate Judiciary Committee Subcommittee on Human
Rights and the Law
Hearing on "Global Internet Freedom and the Rule of Law, Part II"
March 2, 2010**

Chairman Durbin, Ranking Member Coburn, and Members of the Subcommittee.

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

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

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

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

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

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

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

First, our situation in China.

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

Third, the economic implications of censorship.

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

China Update

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

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

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

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

Most recently, in mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China. What at first appeared to be an isolated security incident -- albeit a significant one -- turned out upon investigation to be something quite different.

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

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

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

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

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

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

Other Global Challenges

As I mentioned earlier, Google has become a regular focus of governmental efforts to limit individual expression because our technologies and services enable people with

Internet connections to speak to a worldwide audience. More than 25 governments have blocked Google services over the past few years.

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

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

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

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

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

Economic Implications

The debate on Internet censorship is, of course, not only about human rights. At issue is the continued economic growth spurred by a free and globally accessible Internet.

Barriers to the free flow of information online have significant and serious economic implications: they impose often one-sided restrictions on the services of U.S. and global Internet companies, while also impeding other businesses who depend on the Internet to reach their customers.

When a foreign government pursues censorship policies in a manner that favors domestic Internet companies, this goes against basic international trade principles of non-discrimination and maintaining a level playing field. Local competitors gain a business advantage, and consumers are deprived of the ability to choose the best services for their needs. And when a government disrupts an Internet service in its entirety – e.g., blocking an entire website because of concerns with a handful of user-generated postings – the government is restricting trade well-beyond what would be required even if it had a legitimate public policy justification for the censorship.

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

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

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

How Governments Can Support Free Expression

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

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

First, making every effort at both the grassroots and government level to maximize access to information online. The State Department recently issued a request for proposals on projects to help citizens on the ground access information they would not otherwise be able to share or receive. Google supports the joint commitment of Congress and the Obama Administration to provide funds to groups around the world to

make sure people who need to access the Internet safely get the right training and tools. This is a great step forward, and we believe much more can be done to support grassroots organizations that develop technology to combat Internet censorship.

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

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

We are also grateful for the efforts of lawmakers -- and in particular your leadership Mr. Chairman -- to bring more companies into the Global Network Initiative (GNI).

As a platform for companies, human rights groups, investors, and academics, the GNI requires its members to commit to standards that respect and protect user rights to privacy and freedom of expression. Additional corporate participation will help the GNI reach its full potential -- and we look to the Members of this Committee for continued leadership.

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

On the multilateral human rights front, enforcing and supporting the mechanisms of the International Covenant on Civil and Political Rights and others under the UN system (e.g., the UN Human Rights Committee) to demand accountability from governments for Internet censorship is helpful. At the very least, these mechanisms can be better used to shine light on government abuses.

Conclusion

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

**WRITTEN TESTIMONY OF MORTON SKLAR,
FOUNDING EXECUTIVE DIRECTOR EMERITUS (RETIRED),
WORLD ORGANIZATION FOR HUMAN RIGHTS USA***

**COMPLICITY OF U.S. CORPORATIONS IN INTERNET
HUMAN RIGHTS ABUSES BY THE GOVERNMENT OF CHINA
AND OTHER REPRESSIVE REGIMES**

**SUBMITTED TO THE
SUBCOMMITTEE ON HUMAN RIGHTS AND THE LAW
OF THE JUDICIARY COMMITTEE OF THE U.S. SENATE
HEARING ON MARCH 2, 2010**

Contact: mshumanrights@verizon.net; telephone: (301) 946-4649

*** This testimony is provided in a personal capacity, and does not
necessarily represent the official views of Human Rights USA**

Senator Durbin and Members of the Committee:

The problem that Google brought to public attention a few weeks ago concerning cyber-attacks by Government of China agents against a large number of U.S. government agencies and corporations is just the tip of the iceberg with respect to China's multifaceted electronic monitoring activities that result in major human rights abuses and national security violations, both in their own country, and in the United States. The significant role that U.S. companies have played in facilitating electronic surveillance activities by China and other highly repressive regimes around the world, including Iran, through the provision of Internet user information and the export of products and technologies that build foreign electronic surveillance capacity, should be profoundly troubling for the American people, and deserves considerably more attention than it has received.

To its credit, the U.S. Congress has for a number of years sought to bring attention to this problem. This Committee under the leadership of Chairman Durbin, as well as the House of Representatives Human Rights Subcommittee of the Foreign Affairs Committee under the leadership of the late Congressman Tom Lantos and Co-Chair Chris Smith, have held a series of hearings on these issues, including those held in February, 2006, bringing representatives of Yahoo!, Cisco Systems and other U.S. companies before Congress in an effort to find out more about how their actions and policies are helping to make Internet surveillance and repression possible. These hearings have helped to reveal the sad fact that, in direct violation of U.S. laws, and fed by the profit motive, Yahoo!, Cisco Systems and many other U.S. companies have provided significant support and assistance that has facilitated major human rights Internet abuses in China, and in other repressive regimes such as Iran.

This Committee's hearings of May 20, 2008 revealed that Cisco Systems had marketed and sold Internet routers to Chinese law enforcement agencies with the articulated purpose of helping Chinese officials identify, arrest and persecute political dissidents and religious minorities (Falun Gong practitioners in particular) in violation of U.S. export control laws that prohibit all sales and exports to China that served law enforcement purposes and that could be misused to promote human rights abuses (the Tiananmen Square provisions of the Export Administration Act). Hearings on the House side in November 2007 brought considerable pressure to bear on Yahoo! for improperly providing Internet user information to Chinese authorities that resulted in the arrest of Shi Tao and hundreds of other Chinese who lawfully and peacefully used the Internet for free speech and democracy support purposes. As a result of those hearings, Yahoo! settled a lawsuit filed on behalf of Shi Tao and detainees in Chinese prisons who were arrested and tortured as a result of Yahoo!'s complicity,

brought by the human rights group that I founded and headed for many years (Human Rights USA).

But sad to say, the problem has not been resolved by these several Congressional hearings, the successful Human Rights USA lawsuit, and the substantial media and public attention that has been brought to bear on the issue of the participation and facilitation of major U.S. internet companies like Yahoo! and Cisco in human rights abuses involving the Internet. Neither have any concrete results been achieved through the voluntary effort by several U.S. companies to develop a Code of Conduct for business practices affecting the Internet (the Global Network Initiative). It is noteworthy that Cisco Systems, for one, did not even see the value of participating in the Internet industry Code of Conduct initiative, and has refused to endorse the resulting Code. As has become clear through the hearings of this Committee and through other means, Cisco has been selling Internet equipment and technology to China law enforcement agencies in direct violation of U.S. law and the industry Code of Conduct, and encourages these sales by suggesting that they would enhance China's capability to monitor Internet use and electronic communications so as to identify and track dissidents.

The time has come for the U.S. Congress to act in a more forceful way to make certain that U.S. companies are no longer permitted to facilitate persecution by making electronic surveillance possible through the provision of U.S. products and technologies. Nor should the U.S. Government continue to fail in its duty to properly monitor and enforce the export control laws with respect to Internet technology and human rights abuses. We urge Congress to pursue these types of hearings even more forcefully, and on a broader basis, and to adopt legislation along the lines of the Global Online Freedom Act, that will help to ensure that U.S. companies like Yahoo! and Cisco are not permitted to facilitate major human rights abuses by repressive governments involving the Internet and electronic surveillance.

As we have indicated, the problem is not restricted to U.S. companies such as Yahoo! and Cisco providing Internet information and monitoring technologies to repressive governments in direct violation of U.S. law and ethical standards. The Bureau of Industry and Security of the U.S. Department of Commerce shares responsibility, as they have not properly monitored and enforced compliance with U.S. export control laws – specifically the Tiananmen Square provisions of the Export Administration Act – to identify, prevent, and impose sanctions on violations. Just one week ago BIS issued a new Compliance Guide that for the first time provides much clearer standards for U.S. companies to apply to their marketing and export practices. This was an important first step. But it remains to be seen whether, in practice, the profit motive of the companies, and the balance of trade, political, and foreign policy concerns of the U.S.

Government, will be allowed to override the Tiananmen Square prohibitions and other human rights standards incorporated in U.S. laws and policies.

The situation involving Cisco Systems' sales in China, discussed in the May 20, 2008 hearing of this Subcommittee in which Cisco's General Counsel Mark Chandler appeared and testified under oath before Congress, provides an excellent case in point.

As your hearings indicated, Cisco sells routers and switches to the Chinese government for use in various public sectors including that of the police and security forces. [p. 17 re: PSB]. Cisco has consistently claimed that these are "off the shelf" products that could be purchased elsewhere, and that they are "dual use," or "neutral" products that are not necessarily geared to prohibited uses under U.S. law. However, this overlooks several obvious points. First, Cisco made a determined effort to market these items to law enforcement entities in China, and Cisco geared its sales pitch to the use of these items for law enforcement purposes – specifically, the monitoring of Internet use and electronic communications, which in turn was used to identify and punish political dissidents and religious minorities for their free speech and free exercise of religion rights. As such, these sales efforts and actual exports violated U.S. law on its face, since they are prohibited on an outright basis by the Tiananmen Square provisions of the Export Administration Act.

Second, Cisco was not making these sales pitches and exports to Chinese law enforcement agencies in a vacuum. Even if, for argument's sake, one accepts that Cisco did not market these products specifically for prohibited law enforcement purposes, the company had ample reason to know that Chinese law enforcement agencies were engaging in Internet monitoring activities on a massive scale, and that the sale of these products and technologies could easily be misused to facilitate exactly the type of Internet monitoring and human rights abuses that U.S. laws and policies condemned. A number of highly reliable sources, including the U.S. Department of State in its annual Human Rights Country Reports on China, numerous international human rights organizations, and the media, have been making clear for many years what China was planning and doing with respect to the repressive monitoring of the Internet and electronic communications. Cisco was on full notice, and should have had no doubt about what these products and technologies were going to be used for. Indeed, Cisco's marketing material made clear that they fully realized the unlawful law enforcement purposes that attached to their exports. Turning a blind eye to reality and to the violation of U.S. law that was involved in these sales and exports was not a reasonable or lawful business practice.

Third, the Compliance Guide just issued by the Commerce Department's Bureau of Industry and Security makes clear that a company's obligations to monitor and comply with Export Administration Act requirements and prohibitions go beyond just determining whether the equipment that is the subject of a

proposed sale is listed among the categories and types of products whose exports are restricted. ***Epecially*** where "dual use" types of equipment such as computers and electronic communications products are involved, a company must make a realistic assessment as to the end users and the end use that their products will be associated with. In Cisco's case, the end users were law enforcement agencies in China, and the end use was ***represented and acknowledged by Cisco officials themselves*** as being associated with Internet surveillance activities specifically designed to identify and arrest dissidents. As such, Cisco's actions constituted a *per se* violation of U.S. export control laws.

Just prior to the May 20, 2008 hearing before this subcommittee, an internal Cisco powerpoint presentation relating to a sales pitch to the Chinese government was leaked to the public, in which a Cisco employee took note of the Chinese government's aim to "combat 'Falun Gong' evil religion and other hostilities" and suggested that purchase and use of their product would increase the capability of Chinese law enforcement agencies to monitor Internet use and to identify dissident users. This demonstrates undeniably that Cisco knew that the supposedly neutral or dual use products and technologies it sold and exported to Chinese authorities could easily be used for purposes prohibited by U.S. law, for the surveillance and monitoring of Internet and electronic communications for law enforcement purposes.

Mr. Chandler's responses to questions posed during and after this hearing demonstrated Cisco's cavalier attitude toward its critical role in enabling China to carry out internet-based acts of repression. While Mr. Chandler stated during the hearing that he was "appalled" and "very disappointed" to see such language included in the leaked document [p. 17 of May 20, 2008 hearing transcript], he did not deny that Cisco knew that one purpose of the Chinese Government's Operation Golden Shield project of Internet monitoring was to combat Falun Gong and other religious and political dissidents. [p. 38-39] Moreover, in neither his oral statement nor his written responses was he able to identify any specific ways in which Cisco sought to ensure that China could not use its products in such a way as to undermine human rights. All he could muster was a reference to a very general policy requiring that employees "treat others equally and with respect and dignity." [e.g., pp. 21, 36-37] Similarly, Chandler was unable to indicate that Cisco informs government clients, in writing or otherwise, that Cisco would not assist in efforts toward censorship and repression, nor was he willing to commit the company to doing so in the future. [e.g., pp. 22, 38] Finally, Chandler suggested that Cisco was too large, and conducted too much overseas business to properly monitor the behavior of all its foreign-based employees and affiliates with regard to any support they gave foreign governments in their acts of repression, as evidenced, for example, by Cisco's powerpoint presentation for the Chinese authorities that promoted the sale of Cisco routers for the specific purpose of enhancing Internet monitoring activities. [e.g., p. 39]

As a result of information that has been unearthed by this Committee and by other sources, Cisco's unlawful and unethical sales to the Chinese authorities has been garnering substantial attention over the past few years. Shareholders are demanding through shareholder resolutions and proposals that the company take tangible action to end its involvement in internet-related human rights violations, and adopt institutional procedures and mechanisms to identify and prevent questionable sales that would have negative human rights impacts. For example, Boston Common Asset Management and RiskMetrics Group, representing over 24 million shares of Cisco Systems stock (NASDAQ: CSCO) totaling over \$580 million have submitted a number of shareholders' proposals over the years "to take concrete steps to mitigate human rights related risks that could ultimately stifle long-term demand for the networks it builds (Boston Common release of November 10, 2009 titled: "Investors Representing Over \$580 in Cisco Shares Are Urging Cisco to Respond to Human Rights Risks In Its Global Operations"). They requested more openness from Cisco in providing "additional information in its existing public documents on policies and practices related to doing business with governments that restrict certain human rights," and sought adoption of a policy to refrain from selling products that would aid in repressive actions by foreign governments. They noted that Cisco is "not immune" to risks to the company posed by sales that promote human rights abuses, and that "Cisco's responses to our concerns have been wholly inadequate," according to Adam Kanzer, Managing Director and General Counsel of Domini Social Investments, one of the sponsors of the proposals.

Shareholders have good cause to be concerned about Cisco's China sales, not only from a legal and human rights standpoint but also from a fiscal standpoint. The illegal and imprudent actions of Cisco's leadership in selling products to the Chinese authorities for the use in law enforcement activities, in contravention of the Tiananmen Square Provisions of the Export Control Act, expose the company to a host of negative consequences, all of which jeopardize the company's financial position. The Department of Commerce would be fully justified in bringing both criminal and civil enforcement action against Cisco, potentially resulting in substantial fines and considerable negative publicity for the company. The May 2008 hearings of this Subcommittee focusing on Cisco's human rights violations, and these follow-up hearings today, are only the beginning of the negative public attention that will be coming Cisco's way unless they stop these unlawful and unthinking practices and develop a substantial company-wide policy and compliance mechanism to prevent these human rights abuses in the future. The mounting negative publicity focused on Cisco and its China sales worries shareholders, as it sheds doubt on the capability of the company's leaders to carry out their responsibilities in accordance with the law, and the appropriateness of actions that could cause their investments to decrease in value.

The newly issued BIS Compliance Guide sets out a very compelling explanation of the negative impacts on a company that may well be associated

with improper and unlawful exports of the type we are discussing involving Cisco and China. For example, page 122 of the Guide notes that companies "may be subject to criminal prosecution and/or administrative penalties," and suggests that "Bad publicity alone can cost companies incalculable sums, in terms of future business, not to mention costs associated with lengthy and costly litigation, or administrative or criminal penalties." The Guide makes clear that it is the company's obligation to "be aware of suspicious circumstances and Red Flags that may be present in an export transaction,... [to] evaluate all of the information after inquiry and refrain from engaging in the transaction if the Red Flags cannot be resolved." Cisco's handling of its marketing and exports to China suggests it has not followed these recommended, acceptable good business practices.

What Congress and the U.S. Government Must Do

To this Subcommittee's great credit, in Part I of its hearing involving Cisco in May 2008, it asked Cisco a number of probing questions regarding the details of the company's sales to the Chinese authorities and the ways in which the company ensures that while selling products to repressive regimes it is not complicit in human rights violations carried out by those regimes. Siimilar questions were directed at Cisco in the letters sent by this Committee to various U.S. companies including Cisco notifying them of today's hearings. Regrettably Cisco failed to respond in any meaningful way, and therefore these questions remain unanswered. Going forward, Cisco should be required, at a minimum, to provide this Subcommittee with specific information regarding a number of important topics:

First, in Congressional hearings Cisco has cited to its own company's Code of Conduct as serving to ensure that its employees do not customize Cisco products in such as way as to undermine human rights, or market its services to government authorities in China or any other nation on the basis of their usefulness in detecting, monitoring, or censoring political dissent or expression. Cisco should be required to provide the subcommittee with a copy of its Code of Conduct and any other relevant Cisco documents, particularly those developed after the 2008 subcommittee hearing, highlighting the portions that are relevant to the sale of its products to governments that are known to use them for law enforcement purposes. Cisco also should provide details of all cases where the Code of Conduct and any other relevant standards along these lines have been applied in the past in situations in which sales to China and other repressive regimes have been considered, or have taken place.

Second, Cisco should be required to provide detailed information on any mechanism that it has in place, or is considering, to monitor and assure compliance with its own Code of Conduct, and with U.S. export and human rights laws. Does Cisco have a compliance officer to monitor these issues, or a compliance process in place to assess, in advance, the impacts of sales to countries that are known to use Cisco products for law enforcement and

repressive purposes? Did that officer or process pass judgment on the appropriateness of the decision to market or sell the products under discussion to Chinese law enforcement agencies?

Third, Cisco should specifically identify and describe each and every product and technology that it has exported to China, when these transfers occurred, whether export licenses were applied for, and what specific entities were the recipients and users of each of these products. Additionally, it should address whether the company conducted any sort of process to evaluate potential misuse of the product, or what entities would be the end users, consistent with, or at least along the lines of, the Guidelines on Compliance that BIS has just issued.

Fourth, how many law enforcement marketing shows in China, or involving Chinese law enforcement agencies, has Cisco attended since 2002? How many sales to Chinese law enforcement agencies have taken place since 2002, and what was the nature of the products or technologies sold? What entities were the buyers and recipients of these products?

Without this information – which can only be provided by Cisco – there is no real way to assess the extent to which U.S. export laws have been broken and whether Cisco conducted the appropriate and necessary steps to make sound and lawful business judgments regarding proposed exports when the products and technologies were being marketed and sold to China.

In addition, Congress also must pay much more attention to how and whether the Department of Commerce's Bureau of Industry and Security is doing an adequate job of carrying out its responsibility to monitor and assure compliance with various provisions of the Export Administration Act that have been given short shrift in the past, including the Tiananmen Square human rights prohibitions.

Finally, Congress must not only pass the existing provisions of the proposed Global Online Freedom Act, but must give careful consideration to whether the present draft of that Bill goes far enough in dealing with the emerging issues of U.S. company involvement in major human rights abuses, and cyber attacks by repressive foreign governments and their agents.

Our nation's national security interests, as well as our firm commitment to human rights, demand that we hold our corporate entities accountable in this area, and make sure that U.S. companies do not contribute to or facilitate the repressive and intrusive actions by foreign governments and their agents involving Internet use and electronic communications.



August 1, 2008

The Honorable Senator Richard Durbin
The Honorable Senator Tom Coburn

Dear Senators:

Thank you for your letter of July 21st to Yahoo! CEO Jerry Yang seeking an update on the development of a global code of conduct that Yahoo!, our industry counterparts, human rights advocates, academics, investors, and others are developing to protect and promote human rights globally. Our efforts in this area reflect our collective commitment to freedom of expression and privacy. We look forward to sharing with you more details of the significant progress we have made as a diverse group.

As I testified before you on May 20th, we have participated in an intensive and broad-based effort to develop a global code of conduct for the past eighteen months. We have worked at the most senior levels of our company with representatives from other companies and NGOs to strike the right balance on a voluntary code of conduct – a balance that will help bring the promise of the Internet to ordinary citizens around the globe while protecting their rights to freedom of expression and privacy.

Not long after the May 20th hearing, we achieved a significant collective milestone and reached agreement in principle on the core components of the code of conduct. We all believe the initiative will represent a meaningful, integrated, and sustainable approach to addressing the root causes of the challenges to Internet freedom, and will help the Internet, communications, and technology (ICT) sector protect and advance the fundamental rights to freedom of expression and privacy.

The members of what we have named the “ICT Initiative on Freedom of Expression and Privacy” are now reviewing the agreement for final approval, and we are optimistic that we will launch the Initiative this fall. The core components of the Initiative are:

- o **Principles on Freedom of Expression and Privacy** that provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of freedom of expression and privacy globally. The Principles describe key commitments in the following areas: Freedom of Expression; Privacy; Responsible Company Decision Making; Multi-Stakeholder Collaboration; Governance, Accountability & Transparency.
- o **Implementation Guidelines** that provide further details on how participating companies will put the Principles into practice. The Implementation Guidelines



701 First Avenue • Sunnyvale, CA 94089 • phone 408 349-3300 • fax 408 349-3331

yahoo.com

describe a set of actions which constitute compliance with the Principles and provide companies with guidance on how to implement the Principles.

- o **A Governance, Accountability and Learning Framework** founded on the notion that an organizational and multi-stakeholder governance structure is required to support the Principles and that participating companies should be held accountable for their role in the implementation of the Principles through a system of independent assessment.

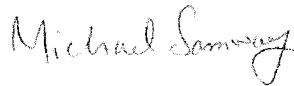
As you made clear in your letter, events around the world make a code of conduct not just ideal but essential, as companies and others work to ensure the protection of basic human rights for citizens across the globe. I assure you that at Yahoo! we are committed to seeing this effort through to a successful conclusion as swiftly as possible, and we believe our ability to offer the tools of the Internet to citizens throughout the world depends on it.

I would also like to reiterate that Yahoo! is not waiting for the launch of the voluntary code of conduct – we are already strengthening Yahoo!'s commitment to global human rights on many fronts. Over the past year, we have redoubled our efforts through the creation of a human rights fund that provides assistance to political dissidents and their families; we have implemented our own formal human rights assessment as we explore challenging markets around the world; and we have established academic fellowships at two major universities to help advance the cause of global human rights. We have also established a dedicated business and human rights program as part of our effort to make responsible decisions in the areas of free expression and privacy globally. Each of our efforts is intended to further our goal of promoting access to information, while simultaneously advancing individual rights worldwide.

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 also believe the most powerful forces to help change the policies and practices of governments around the world often reside within our own government. Jerry Yang has personally asked Secretary Rice and her colleagues at the State Department to redouble diplomatic efforts that advance the cause of individual freedoms, particularly in anticipation of the Olympics, and we hope that you and your colleagues will continue to encourage these efforts as well.

We are grateful for your continued focus on Internet freedom, and look forward to working with you as Yahoo! continues pursuing a global leadership role in the field of business and human rights.

Sincerely,



Michael Samway
Vice President & Deputy General Counsel, Yahoo! Inc.

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

July 21, 2008

Dr. Jerry Yang
Chief Executive Officer
Yahoo! Inc
701 First Avenue
Sunnyvale, California 94089

Dear Dr. Yang:

We write to request an update on the voluntary code of conduct for internet companies that Yahoo! and other stakeholders are developing.

We discussed the code of conduct with Yahoo! Vice President and Deputy General Counsel Michael Samway during "Global Internet Freedom: Corporate Responsibility and the Rule of Law," a May 20, 2008 hearing of the U.S. Senate Subcommittee on Human Rights and the Law. As we discussed during the hearing, it is critical to the protection of fundamental human rights that a voluntary code of conduct be finalized and implemented as soon as possible.

During the hearing, Mr. Samway assured us that finalizing the code was a priority for Yahoo!, but it has been almost two months since the hearing and eighteen months since Yahoo! and other participants began to develop the code. We recognize that the code of conduct raises complicated issues with potentially far-reaching effects on your company's operations, but with every day that the code is not finalized the human rights of people across the globe are jeopardized.

We are especially concerned that the code of conduct is not yet completed because the Olympic Games will begin in China in three weeks. Without a code of conduct in place, it is more likely that Yahoo! and other American internet companies will be pressured by the Chinese government to provide sensitive personal information regarding American athletes, journalists and tourists who use the internet while they are in China during the Olympics. Moreover, in the absence of a code of conduct, it is unclear how Yahoo! and other American internet companies might respond to requests from the Chinese government and other repressive regimes to censor political or religious content.

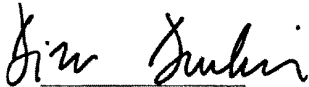
It is also important to note that the failure to finalize a code of conduct suggests that it may be necessary for Congress to consider legislation to ensure that American companies operating in internet-restricting countries protect user privacy and freedom of expression. As Senator Durbin said during the hearing, if American internet companies are unable to regulate themselves effectively, Congress may be forced to consider doing so.

At the hearing, there was agreement that Yahoo! and other American internet companies operating in internet-restricting countries should promote free speech and not facilitate

repression. A voluntary code of conduct would be one important step toward our shared goals of promoting freedom of expression and protecting the privacy of internet users around the world.

Given the importance of this issue, we would appreciate a response to this letter as soon as possible and no later than August 1, 2008. Thank you for your time and consideration.

Sincerely,


Richard J. Durbin


Tom Coburn

○