THE INTERNET IN CHINA: A TOOL FOR FREEDOM OR SUPPRESSION?

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON AFRICA, GLOBAL HUMAN RIGHTS AND INTERNATIONAL OPERATIONS

AND THE

SUBCOMMITTEE ON ASIA AND THE PACIFIC

OF THE

COMMITTEE ON INTERNATIONAL RELATIONS HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

FEBRUARY 15, 2006

Serial No. 109–157

Printed for the use of the Committee on International Relations

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

U.S. GOVERNMENT PRINTING OFFICE

26–075PDF WASHINGTON : 2006

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON INTERNATIONAL RELATIONS

HENRY J. HYDE, Illinois, *Chairman*

JAMES A. LEACH, Iowa
CHRISTOPHER H. SMITH, New Jersey, *Vice Chairman*
DAN BURTON, Indiana
ELTON GALLEGLY, California
ILEANA ROS-LEHTINEN, Florida
DANA ROHRABACHER, California
EDWARD R. ROYCE, California
PETER T. KING, New York
STEVE CHABOT, Ohio
THOMAS G. TANCREDO, Colorado
RON PAUL, Texas
DARRELL ISSA, California
JEFF FLAKE, Arizona
JO ANN DAVIS, Virginia
MARK GREEN, Wisconsin
JERRY WELLER, Illinois
MIKE PENCE, Indiana
THADDEUS G. McCOTTER, Michigan
KATHERINE HARRIS, Florida
JOE WILSON, South Carolina
JOHN BOOZMAN, Arkansas
J. GRESHAM BARRETT, South Carolina
CONNIE MACK, Florida
JEFF FORTENBERRY, Nebraska
MICHAEL McCAUL, Texas
TED POE, Texas
TOM LANTOS, California
HOWARD L. BERMAN, California
GARY L. ACKERMAN, New York
ENI F.H. FALEOMAVAEGA, American Samoa
DONALD M. PAYNE, New Jersey
SHERROD BROWN, Ohio
BRAD SHERMAN, California
ROBERT WEXLER, Florida
ELIOT L. ENGEL, New York
WILLIAM D. DELAHUNT, Massachusetts
GREGORY W. MEEKS, New York
BARBARA LEE, California
JOSEPH CROWLEY, New York
EARL BLUMENAUER, Oregon
SHELLEY BERKLEY, Nevada
GRACE F. NAPOLITANO, California
ADAM B. SCHIFF, California
DIANE E. WATSON, California
ADAM SMITH, Washington
BETTY McCOLLUM, Minnesota
BEN CHANDLER, Kentucky
DENNIS A. CARDOZA, California
VACANT

THOMAS E. MOONEY, SR., *Staff Director/General Counsel*
ROBERT R. KING, *Democratic Staff Director*

SUBCOMMITTEE ON AFRICA, GLOBAL HUMAN RIGHTS AND INTERNATIONAL OPERATIONS

CHRISTOPHER H. SMITH, New Jersey, *Chairman*

THOMAS G. TANCREDO, Colorado
JEFF FLAKE, Arizona
MARK GREEN, Wisconsin
JOHN BOOZMAN, Arkansas
JEFF FORTENBERRY, Nebraska
EDWARD R. ROYCE, California, *Vice Chairman*
DONALD M. PAYNE, New Jersey
GREGORY W. MEEKS, New York
BARBARA LEE, California
DIANE E. WATSON, California
BETTY MCCOLLUM, Minnesota
EARL BLUMENAUER, Oregon

MARY M. NOONAN, *Subcommittee Staff Director*
GREG SIMPKINS, *Subcommittee Professional Staff Member*
NOELLE LUSANE, *Democratic Professional Staff Member*
SHERI A. RICKERT, *Subcommittee Professional Staff Member and Counsel*
LINDSEY M. PLUMLEY, *Staff Associate*

SUBCOMMITTEE ON ASIA AND THE PACIFIC

JAMES A. LEACH, Iowa, *Chairman*

DAN BURTON, Indiana, *Vice Chairman*
ELTON GALLEGLY, California
DANA ROHRABACHER, California
STEVE CHABOT, Ohio
RON PAUL, Texas
JOE WILSON, South Carolina
ENI F. H. FALEOMAVAEGA, American Samoa
SHERROD BROWN, Ohio
EARL BLUMENAUER, Oregon
ADAM SMITH, Washington
GARY L. ACKERMAN, New York
BRAD SHERMAN, California

JAMES W. MCCORMICK, *Subcommittee Staff Director*
LISA M. WILLIAMS, *Democratic Professional Staff Member*
DOUGLAS ANDERSON, *Professional Staff Member & Counsel*
TIERNEN M. DONALD, *Staff Associate*

CONTENTS

THE INTERNET IN CHINA: A TOOL FOR FREEDOM OR SUPPRESSION?

WEDNESDAY, FEBRUARY 15, 2006

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON AFRICA, GLOBAL HUMAN RIGHTS
AND INTERNATIONAL OPERATIONS,
SUBCOMMITTEE ON ASIA AND THE PACIFIC,
COMMITTEE ON INTERNATIONAL RELATIONS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10 o'clock a.m. in room 2172, Rayburn House Office Building, Hon. Christopher H. Smith of New Jersey [Chairman of the Subcommittee on Africa, Global Human Rights and International Operations] presiding, and James A. Leach [Chairman of Subcommittee on Asia and the Pacific] present.

Mr. SMITH OF NEW JERSEY. The Committee will come to order. Good morning and welcome to this hearing on the Internet in China. We are here to examine a problem that is deeply troubling to me and, I believe, to the American people, and that is that American technology and know-how is substantially enabling repressive regimes in China and elsewhere in the world to cruelly exploit and abuse their own citizens.

Over the years, I have held and chaired 25 hearings on human rights abuses in China, and while China's economy has improved somewhat, the human rights situation remains abysmal. So-called "economic reform" has utterly failed to result in the protection of freedom of speech, expression, or assembly. The Laogai system of forced labor camps is still full to capacity, with an estimated 6 million people; the Chinese Government which permits a horrifying trade in human organs continues unabated; the PRC's draconian, one-child-per-couple policy has made brothers and sisters illegal and coerced abortion commonplace; and political and religious dissidents are systematically persecuted and tortured.

Similarly, while the Internet has opened up commercial opportunities and provided access to vast amounts of information for people the world over, the Internet has also become a malicious tool, a cyber-sledgehammer of repression of the Government of the People's Republic of China. As soon as the promise of the Internet began to be fulfilled, when brave Chinese began to e-mail each other around the world about human rights issues and corruption by government leaders, the party cracked down. To date, an estimated 49 cyber-dissidents and some 32 journalists have been imprisoned by the PRC for merely posting information on the Internet

critical of the regime. And, frankly, that is likely to be only the tip of the iceberg.

Tragically, history shows us that American companies and their subsidiaries have provided the technology to crush human rights in the past. Edwin Black's book, *IBM and the Holocaust*, reveals the dark story of IBM's strategic alliance with Nazi Germany. Thanks to IBM's enabling technologies, from programs for identification and cataloging to the use of IBM's punch card technology, Hitler and the Third Reich were able to automate the genocide of the Jews. And I would recommend to anyone who is interested to read this book. It is a very, very incisive commentary on how that collaboration worked.

U.S. technology companies today are engaged in a similar sickening collaboration, decapitating the voice of the dissidents. In 2005, Yahoo!'s cooperation with Chinese secret police led to the imprisonment of cyber-dissident Shi Tao. And this was not the first time. According to Reporters Without Borders, Yahoo! also handed over data to Chinese authorities on another of its users, Li Zhi. Li Zhi was sentenced on December 10, 2003, to 8 years in prison for inciting subversion. His "crime" was criticizing in online discussion groups and articles the well-known corruption of local officials.

Women and men are going to the gulag and being tortured as a direct result of information handed over to Chinese officials. When Yahoo! was asked to explain its actions, Yahoo! said that it must adhere to local laws in all countries where it operates. But my response to that is, if the secret police, a half century ago, asked where Anne Frank was hiding, would the correct answer be to hand over the information in order to comply with local laws? Again, these are not victimless crimes that the Chinese secret police are committing, and I believe we must stand with the oppressed and not with the oppressors.

I was recently on a news show talking about Google and China. The question was asked, "Should it be business's concern to promote democracy in foreign nations?" While that would be great, that is not necessarily the right question. The more appropriate question today is, "Should businesses enable the continuation of repressive dictatorships by partnering with a corrupt and cruel secret police and by cooperating with laws that violate basic human rights?"

I believe that two of the most essential pillars that prop up totalitarian regimes are the secret police and propaganda. Yet for the sake of market share and profits, leading U.S. companies, like Google, Yahoo!, Cisco, and Microsoft, have compromised both the integrity of their product and their duties as responsible corporate citizens. They have, indeed, aided and abetted the Chinese regime to prop up both of these pillars, secret police and propaganda, propagating the message of the dictatorship unabated and supporting the secret police in a myriad of ways, including surveillance and invasion of privacy, in order to effectuate the massive crackdown on its citizens.

Through an approach that monitors, filters, and blocks content with the use of technology and human monitors, the Chinese people have little access to uncensored information about any political or human rights topic, unless, of course, Big Brother wants you to

see it. Google.cn, China's search engine, is guaranteed to take you to the virtual land of deceit, disinformation, and the big lie. As such, the Chinese Government utilizes the technology of United States IT companies combined with human censors, led by an estimated force of 30,000 cyber police, to control information in China.

Web sites that provide the Chinese people with news about their country and the world, such as the BCC, much of CCN, as well as Voice of America and Radio Free Asia, are routinely blocked in China. In addition, when a user enters a forbidden word, such as "democracy" or "Chinese torture" or "Falun Gong," the search results are blocked, or you are redirected to a misleading site, and the user's computer can be frozen for unspecified periods of time.

Cisco has provided the Chinese Government with the technology necessary to filter Internet content through its creation of Police Net, one of the tools the regime uses to control the Internet. Cisco holds 60 percent of the Chinese market for routers, switches, and other sophisticated networking gear, and its estimated revenue from China, according to Derek Bambauer of Legal Affairs, is estimated to be $500 million annually. Yet Cisco has also done little creative thinking to try to minimize the likelihood that its products will be used repressively, such as limiting eavesdropping abilities to specific computer addresses.

Similarly, Google censors what is euphemistically called "politically sensitive" terms like "democracy," "China human rights," and "China torture" on the new Chinese search site, Google.cn. Let us take a look at what that means in practice. A search for terms such as "Tiananmen Square" produces two very different results. The one from Google.cn shows a picture of a smiling company, but the results from Google.com show scores of photos depicting the mayhem and brutality of the 1989 Tiananmen Square massacre.

Another example: Let us look at "China and torture." Google has said that some information is better than nothing, but in this case, the limited information displayed amounts to disinformation. A half truth is not the truth; it is a lie, and a lie is worse than nothing. It is hard not to draw the conclusion that Google has seriously compromised its "Don't Be Evil" policy. Indeed, it has become evil's accomplice, and hopefully that will change.

Not surprisingly, Americans, not just Chinese, are also victims of this censorship. On an informal request from the Chinese Government, Microsoft, on December 30, 2005, shut down the blog of Zhao Jing because the content of Zhao's blog on MSN Spaces was offensive to the PRC. This hearing, no doubt, is offensive to the PRC, and the Chinese people will never hear about this either.

Zhao had tried to organize a walk-off of journalists at the *Beijing News* after their editor was fired for reporting on clashes between Chinese citizens and police in southern China. However, Microsoft shut down the blog not only in China but everywhere. It not only censored Chinese access to information but American access to information, a step that it only recently pulled back from. Like Yahoo!, MSN defended its decision by asserting that MSN is committed to complying with "local laws, norms, and industry practices in China." Regrettably, I have been unable to find an MSN statement on its commitment to global human rights laws, norms, and industry practices that do promote fundamental human rights.

I can tell you, ladies and gentlemen, standing for human rights has never been easy. It is never without cost. It seems that companies have always resisted having to abide by ethical standards, yet we have seen the success of such agreements as the Sullivan principles in South Africa and the MacBride principles in Northern Ireland.

I, and many of my colleagues on both sides of the aisle, would welcome leadership by the corporations to develop a code of conduct which would spell out how they could operate in China and other repressive countries like Vietnam while not harming citizens and respecting human rights. But I believe our Government also has a major role to play in this critical area and that a more comprehensive framework is needed to protect and promote human rights, and that is why I intend to introduce the Global Online Freedom Act of 2006 within the next couple of days to promote freedom of expression on the Internet.

Let me also point out that there are some encouraging and innovative public and private efforts already underway in this area. Electronic Frontier Foundation, for example, allows Windows-based computers to become proxies for Internet users, circumventing local Internet restrictions. Through the efforts of the U.S. Broadcasting Board of Governors fund of a mere $100,000, VOA and Radio Free Asia's Web sites are accessible to Chinese Internet users through proxy servers because of the technology of Dynaweb and UltraReach.

Earlier this month, the technology firm, Anonymizer, announced that it is developing a new, anticensorship technology that will enable Chinese citizens to safely access the entire Internet, filter free. The solution will be to provide a regularly changing URL so that users can likely access the uncensored Internet, although nothing is guaranteed. In addition, users' identities are apparently protected from online monitoring by the Chinese regime. Lance Cottrell of the company has said it "is not willing to sit idly by while the freedom of the Internet is slowly crushed. We take pride in the fact," he went on to say, "that our online privacy and security solutions provide access to global information for those under the thumb of repressive regimes."

In conclusion, I hope this hearing might also be the beginning of a different sort of dialogue: A discussion on how high-tech firms can partner with the U.S. Government and human rights activists all over the globe to bring down the Great Firewall of China or firewalls anywhere else where there is a repressive country, and on how America's greatest software engineers can use their intelligence to create innovative, new products to protect dissidents rather than to provide the dragnet to capture, to incarcerate, and to torture these dissidents, and, of course, to promote human rights.

I would now like to yield to the distinguished Ranking Member, a good friend and colleague from California who is also a leader in human rights and a leader on this issue, my friend, Tom Lantos, for any time he may desire.

[The prepared statement of Mr. Smith of New Jersey follows:]

PREPARED STATEMENT OF THE HONORABLE CHRISTOPHER H. SMITH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY AND CHAIRMAN, SUBCOMMITTEE ON AFRICA, GLOBAL HUMAN RIGHTS AND INTERNATIONAL OPERATIONS

Good morning and welcome to this hearing on the Internet in China. We are here to examine a problem that is deeply troubling to me, and I believe, to the American people: that American technology and know-how is substantially enabling repressive regimes in China and elsewhere in the world to cruelly exploit and abuse their own citizens.

Over the years, I have held 25 hearings on human rights abuses in China, and while China's economy has improved somewhat, the human rights situation remains abysmal. So-called economic reform has utterly failed to result in the protection of freedom of speech, expression, or assembly. The Laogai system of forced labor camps is still full with an estimated 6 million people; the Chinese government permits a horrifying trade in human organs; the PRC's draconian one-child per couple policy has made brothers and sisters illegal and coerced abortion commonplace; and political and religious dissidents are systematically persecuted and tortured.

Similarly, while the internet has opened up commercial opportunities and provided access to vast amounts of information for people the world over, the internet has also become a malicious tool: a cyber sledgehammer of repression of the government of China. As soon as the promise of the Internet began to be fulfilled—when brave Chinese began to email each other and others about human rights issues and corruption by government leaders—the Party cracked down. To date, an estimated 49 cyber-dissidents and 32 journalists have been imprisoned by the PRC for merely posting information on the Internet critical of the regime. And that's likely to be only the tip of the iceberg.

Tragically, history shows us that American companies and their subsidiaries have provided the technology to crush human rights in the past. Edwin Black's book *IBM and the Holocaust* reveals the dark story of IBM's strategic alliance with Nazi Germany. Thanks to IBM's enabling technologies, from programs for identification and cataloging to the use of IBM's punch card technology, Hitler and the Third Reich were able to automate the genocide of the Jews.

U.S. technology companies today are engaged in a similar sickening collaboration, decapitating the voice of the dissidents. In 2005, Yahoo's cooperation with Chinese secret police led to the imprisonment of the cyber-dissident Shi Tao. And this was not the first time. According to Reporters Without Borders, Yahoo also handed over data to Chinese authorities on another of its users, Li Zhi . Li Zhi was sentenced on December 10, 2003 to eight years in prison for "inciting subversion." His "crime" was to criticize in online discussion groups and articles the well-known corruption of local officials.

Women and men are going to the gulag and being tortured as a direct result of information handed over to Chinese officials. When Yahoo was asked to explain its actions, Yahoo said that it must adhere to local laws in all countries where it operates. But my response to that is: if the secret police a half century ago asked where Anne Frank was hiding, would the correct answer be to hand over the information in order to comply with local laws? These are not victimless crimes. We must stand with the oppressed, not the oppressors.

I was recently on a news show talking about Google and China. The question was asked, "Should it be business' concern to promote democracy in foreign nations?" That's not necessarily the right question. The more appropriate question today is, "Should business enable the continuation of repressive dictatorships by partnering with a corrupt and cruel secret police and by cooperating with laws that violate basic human rights?"

I believe that two of the most essential pillars that prop up totalitarian regimes are the secret police and propaganda. Yet for the sake of market share and profits, leading U.S. companies like Google, Yahoo, Cisco and Microsoft have compromised both the integrity of their product and their duties as responsible corporate citizens. They have aided and abetted the Chinese regime to prop up both of these pillars, propagating the message of the dictatorship unabated and supporting the secret police in a myriad of ways, including surveillance and invasion of privacy, in order to effectuate the massive crackdown on its citizens.

Through an approach that monitors, filters, and blocks content with the use of technology and human monitors, the Chinese people have little access to uncensored information about any political or human rights topic, unless of course, Big Brother wants them to see it. Google.cn, China's search engine, is guaranteed to take you to the virtual land of deceit, disinformation and the big lie. As such, the Chinese government utilizes the technology of U.S. IT companies combined with human censors—led by an estimated force of 30,000 cyber police—to control information in

China. Websites that provide the Chinese people news about their country and the world, such as BBC, much of CNN, as well as Voice of America and Radio Free Asia, are regularly blocked in China. In addition, when a user enters a forbidden word, such as "democracy," "China torture" or "Falun Gong," the search results are blocked, or you are redirected to a misleading site, and the user's computer can be frozen for unspecified periods of time.

Cisco has provided the Chinese government with the technology necessary to filter internet content through its creation of Policenet, one of the tools the regime uses to control the internet. Cisco holds 60 percent of the Chinese market for routers, switches, and other sophisticated networking gear, and its estimated revenue from China, according to Derek Bambauer of *Legal Affairs*, is estimated to be $500 million annually. Yet Cisco has also done little creative thinking to try to minimize the likelihood that its products will be used repressively, such as limiting eavesdropping abilities to specific computer addresses.

Similarly, Google censors what are euphemistically called "politically sensitive" terms, such as "democracy," "China human rights," "China torture" and the like on its new Chinese search site, Google.cn. Let's take a look at what this means in practice. A search for terms such as "Tiananmen Square" produces two very different results. The one from Google.cn shows a picture of a smiling couple, but the results from Google.com show scores of photos depicting the mayhem and brutality of the 1989 Tiananmen square massacre. Another example: let's look at "China and torture." Google has said that some information is better than nothing. But in this case, the limited information displayed amounts to disinformation. A half truth is not the truth—it is a lie. And a lie is worse than nothing. It is hard not to draw the conclusion that Google has seriously compromised its "Don't Be Evil" policy. It has become evil's accomplice.

Not surprisingly, Americans, not just Chinese, are also the victims of this censorship. On an informal request from the Chinese government, Microsoft on December 30, 2005 shut down the blog of Zhao Jing because the content of Zhao's blog on MSN Spaces was offensive to the PRC. Zhao had tried to organize a walk-off of journalists at the *Beijing News* after their editor was fired for reporting on clashes between Chinese citizens and police in southern China. However, Microsoft shut down the blog not only in China, but everywhere. It not only censored Chinese access to information, but American access to information, a step it has only recently pulled back from. Like Yahoo, MSN defended its decision by asserting that MSN is committed to complying with "*local* laws, norms, and industry practices in China." Regrettably, I haven't been able to find an MSN statement on its commitment to *global* laws, norms, and industry practices protecting human rights in China.

Standing for human rights has never been easy or without cost. It seems that companies have always resisted having to abide by ethical standards, yet we have seen the success of such agreements as the Sullivan principles in South Africa and MacBride principles in Northern Ireland. I, and many of my colleagues on both sides of the aisle, would welcome leadership by the corporations to develop a code of conduct which would spell out how they could operate in China and other repressive countries while not harming citizens and respecting human rights. But I believe our government also has a major role to play in this critical area, and that a more comprehensive framework is needed to protect and promote human rights. This is why I intend to introduce The Global Online Freedom Act of 2006 in the coming week to promote freedom of expression on the internet.

There are some encouraging and innovative public and private efforts already underway in this area. Electronic Frontier Foundation, for instance, allows Windows-based computers to become proxies for internet users, circumventing local Internet restrictions. Through the efforts of the U.S. Broadcasting Board of Governors' fund of a mere $100,000, VOA and Radio Free Asia's websites are accessible to Chinese internet users through proxy servers because of the technology of Dynaweb and UltraReach.

Earlier this month, the technology firm Anonymizer announced that it is developing a new anti-censorship technology that will enable Chinese citizens to safely access the entire Internet filter-free. The solution will provide a regularly changing URL so that users can likely access the uncensored internet. In addition, users' identities are apparently protected from online monitoring by the Chinese regime. Lance Cottrell of Anonymizer said it "is not willing to sit idly by while the freedom of the Internet is slowly crushed. We take pride in the fact that our online privacy and security solutions provide access to global information for those under the thumb of repressive regimes."

In conclusion, I hope this hearing might be the beginning of a different sort of dialogue—a discussion on how American high-tech firms can partner with the U.S. government and human rights activists to bring down the Great Firewall of China,

and on how America's greatest software engineers can use their intelligence to create innovative new products to protect dissidents and promote human rights.

John Aird Statement

I would like to take this opportunity to recognize and honor the work of Dr. John S. Aird, a distinguished American whose immeasurable contributions as a scholar, population expert, and defender of human rights have changed the lives of so many over the course of his career.

It was with great sadness that I learned of Dr. Aird's death last October. His passing represents a grave loss for all of us who are committed to ensuring human rights around the world, and his tremendous work in this and other fields will not be forgotten.

Dr. Aird, former Senior Research Specialist on China at the U.S. Census Bureau, served for 28 years as that organization's resident expert on the population of China. He was a forthright and vehement critic of the Chinese government's coercive one-child family planning policy.

During his retirement, Dr. Aird worked as a full-time volunteer. He provided expert testimony in immigration courts for 415 families, helping Chinese citizens fleeing their country's coercive family planning programming to secure asylum in the United States.

John S. Aird was truly one of the most informed and outspoken opponents of China's one-child policy. He testified before this and other Congressional committees on numerous occasions, and I believe my colleagues would join me in saying that his insights were consistently persuasive and well-considered, and proved invaluable to our work on human rights in China.

I would also like to acknowledge today the presence of Dr. Aird's wife of more than 58 years, Mrs. Laurel J. Aird, who has graciously joined us for this important hearing which will continue the course on human rights in China that Dr. Aird helped to chart with his work.

Mr. LANTOS. Thank you very much, Mr. Chairman. I want to commend you for an outstanding, comprehensive statement, and I want to express my appreciation to Chairman Leach and you for affording me the opportunity to say a few words.

Before I come to my foremost statement, let me stipulate for the record the obvious. We work with China on a wide range of issues, ranging from North Korea to Iran, and I very much welcome the opportunity of working with this new and emerging superpower.

Let me also say that I am fully aware of the very important, positive developments that the high-tech companies brought to China. But that is not the topic of our discussion this morning.

The hi-tech companies before the Committee today—Yahoo!, Microsoft, Cisco, and Google—are truly the best in the business. In our open and democratic system, based on our Constitutional guarantee of freedom of expression, these firms have thrived, and their founders have amassed enormous wealth, enormous influence, enormous prestige, but apparently very little social responsibility. Instead of using their power and creativity to bring openness and free speech to China, they have caved in to Beijing's outrageous but predictable demands simply for the sake of profits.

These captains of industry should have been developing new technologies to bypass the sickening censorship of government and repugnant barriers to the Internet. Instead, they enthusiastically volunteered for the Chinese censorship brigade. After initially resisting appearing before Congress, representatives of these companies have come to us today to share their side of things. While some of these firms have been operating in China for years, they have suddenly discovered the need for high-sounding documents which simultaneously affirm their respect for freedom of communication and, at the same time, their complete compliance with repressive laws in China.

In the future, when you type the word "oxymoron" in a search engine, you will find the names of Google, Microsoft, Yahoo!, and Cisco. These companies need to do more than show "virtual" backbone. What Congress is looking for is real spine and a willingness to stand up to the outrageous demands of a totalitarian regime. My message to these companies today is simple. Your abhorrent activities in China are a disgrace. I simply do not understand how your corporate leadership sleeps at night.

Let me start with Yahoo!. As we meet today, Chinese citizens who have the courage to speak their minds on the Internet are in the Chinese gulag because Yahoo! chose to reveal their identities to the Chinese Government. It is bad enough that Beijing is so petrified of dissent that it throws dissidents behind bars for years on end and blacklists their families. But it is beyond comprehension that an American company would play the role of willing accomplice in the Chinese suppression apparatus.

Google and Microsoft similarly argue that they must comply with Chinese laws that prohibit online discussions and searching of certain "sensitive subjects." So they have elected to become surrogate government censors, removing content and blocking information that offends the exquisite political sensitivities of the ruling elite in Beijing. Google often cites its adherence to German laws that prohibit neo-Nazi propaganda. This value-free excuse truly sickens me. Germany is a political democracy, and its freely elected leaders prohibited the hate mongering that three generations ago led to Auschwitz. To pretend to argue that this is analogous to the Chinese situation is beneath contempt.

China has a rubber-stamp Parliament, and the Chinese Government places severe, uncompromising restrictions on freedom of speech and religious liberty. For Google's leaders, who made billions in a free and open society, to become Beijing's censors and agents of repression is unconscionable. They clearly have no moral dilemmas while censoring the suppressed Tibetans and members of the Falun Gong, both persecuted minorities in China. Do these companies have any standards at all?

If tomorrow another repressive government demands that Google block all access to women who want to use e-mail or blogs, will Google comply? What about a Sudanese request to block information on the ongoing genocide in Darfur?

These companies tell us that they will change China, but China has already changed them. Despite their protestations, their suddenly-concocted statements of principle, and an avalanche of press releases, it is clear to all objective observers that if we in Congress had not shined the spotlight on their collusion with Chinese censors, these companies would have continued their nauseating collaboration with a regime of repression. They need to stand with us and fight oppression in China and everywhere where they intend to do business. Thank you, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. Thank you very much, Mr. Lantos. The Chair recognizes Chairman Leach.

Mr. LEACH. Thank you, Mr. Chairman. I am pleased to join you in convening this hearing, and I would just like to note, in addition to chairing the Asia Subcommittee, I Co-Chair the Congressional Executive Commission on China. I raise this because I would like

to note the ground-breaking work that the commission's staff has done on the China Internet issue during the past 4 years. They have assembled an unparalleled data base of English-language resources, including human rights reporting and translations of applicable Chinese laws and regulations which are available on the front page of the commission Web site, which is cecc.gov. I commend these materials to the attention of my colleagues and members of the public who are interested in an understanding of these issues.

As highlighted in the commission's annual report, Chinese citizens face increased government regulation of the Internet, and as we all know, censorship is seldom helpful to any society. We live in an era in which the advancement of human understanding and the growth of the global economy cannot operate effectively without the broadest possible dissemination of knowledge. Ultimately, the Chinese Government may not be able to stem the tide of information unleashed by new technologies and by the growing expectations and sophistication of its own public, but in the meantime, the situation of freedom of expression in China remains problematic.

This may be a particularly awkward week for the United States to raise human rights concerns about another country, given the UN draft report on Guantanamo as well as the continued ramification of instances at Abu Ghraib, but, nonetheless, there are issues in United States-China relations that cannot be ducked, particularly when they involve the responsibilities of U.S. corporations.

During the past year, the Chinese Communist Party has improved its ability to silence and control political discussion on the Internet. Public security authorities have detained and imprisoned dozens of journalists, editors, and writers and shut down one-quarter of the private Web sites in China for failing to register with the government. These actions by Chinese officials have implications not only for China but also for the integrity of the Internet itself as a worldwide forum allowing the free and instantaneous exchange of information.

According to China's own state-run media, it has put together the world's most extensive and comprehensive regulatory system for Internet administration and has perfected a 24-hour, real-time, situational censorship mechanism. A Chinese Government delegate to the UN Working Group on Internet Governance has even been quoted as hoping that China's experience can act as a lesson for the global Internet governance.

These issues bear directly on the development of the rule of law within China. Article 35 of the Chinese Constitution guarantees Chinese citizens freedom of speech and of the press. Any restrictions to these Constitutional rights should be openly legislated and transparently applied. In reality, restrictions imposed by officials are premised upon ill-defined concepts of social stability, state security, and sedition that mask what is, in fact, mere intolerance of dissent.

Interestingly, it was reported yesterday that a number of senior Chinese ex-officials, including Mao's secretary and a former editor in chief of the People's Daily, have courageously issued a public letter warning that depriving the public of freedom of expression will sow the seeds of disaster for a peaceful political transformation in

China. The international community should forge a common voice to urge the Chinese Government to cease its political censorship of the Internet. In this regard, Secretary of State Rice's announcement yesterday that she is establishing a new, global, Internet freedom task force appears to be a constructive initiative.

In this context, some American technology companies have been the focus of recent public attention because of allegations that they have become complicit in the restrictive activities of the Chinese security apparatus. Industry representatives have volunteered to appear today, and this Committee looks forward to hearing their perspective.

I understand that much of the technical architecture of the Internet is substantively agnostic. The same capacities that enable network administrators to protect systems against destructive viruses and allow parents to protect their children from pornography also potentially enable political censorship and the monitoring of dissidents. As with so many technologies, the potential for good or ill depends largely on the intent of the user. Thus, the challenge is to maintain the promise of the technology while also refusing to internalize the intent of those who would use those capacities to restrict the parameters of discussion based on its peaceful political intent.

From this perspective, certain corporate activities appear at first blush to be difficult. For example, it is problematic to see how altering one's search engine to exclude politically sensitive materials is anything other than voluntary cooperation in content-based censorship by Chinese authorities. The same would appear to be true for the removal or blocking of politically sensitive Web blogs or other documents. The potential conflict between censorship and the provision of alternative news is perhaps most acute with regard to Radio Free Asia and Voice of America.

On a human level, the moral hazard of locating Internet operations inside China are most visible in the cases of Li Zhi and Shi Tao, online writers who were sentenced to 8 and 10 years, respectively, after information allegedly provided by one Internet service provider reportedly enabled Chinese authorities to personally identify and publish them. Such activities have coercive ramifications for individuals and individual rights in China and unhealthful ramifications for advancing the rule of law in that country.

What is interesting in the censorship practices of American companies is that the censorship practices of American companies do not represent attempts to uphold the rhetoric of the Chinese Constitution. Rather, they are undertaken in response to, or in anticipation of, a threat of commercial or criminal reprisals by the Chinese Government which contravene their own Constitution.

It is presently impossible to gauge the leverage that American companies possess inside China because many of the limitations they observed are self-imposed and were apparently influenced by but not negotiated with Chinese authorities. By preemptively altering their online products to conform with the predilections of Chinese censors, those companies may be diluting the liberalizing pressure created by the desire of the Chinese people to use their original, unaltered products.

To note one example, when China temporarily shut down access to Google.com, a significant public outcry developed which helped

lead to the eventual restoration of that search service. I worry that by providing a sanitized, sensitized version of Google, that company may be allowing Chinese censors to avoid the public pressure that otherwise would result from their restriction decisions.

Citizens of China are willing to risk jail for freedom of expression when certain American companies are unwilling to risk profits for the same principles.

In conclusion, the Internet is an unprecedented tool for the advancement and utilization of knowledge. American search engines and content hosts are considered the most sophisticated in the world. All of us, governments and industries and concerned citizens, should work together to ensure that citizens of China and elsewhere are not denied access to these tools. Thank you, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. Chairman Leach, thank you so very much for that very eloquent statement.

The Chair recognizes the Ranking Member from American Samoa, Mr. Faleomavaega.

Mr. FALEOMAVAEGA. Thank you, Mr. Chairman. I also want to commend you and Chairman Leach for calling this joint hearing together and certainly compliment our senior Ranking Member on our Committee, Mr. Lantos, for his eloquent statement.

Mr. Chairman, before I proceed also with my formal statement as I have prepared this morning, I just want to offer a couple of observations, if I may, in terms of the statements that have been presented before our joint Subcommittee hearing this morning.

If there is one word that I offer my sense of what limited knowledge that I have and understanding of the situation that we are faced with not only in China but throughout the Asia-Pacific region, I suppose as someone who is a Member of this Committee who probably is the only Member of the Committee whose roots is from the Asia-Pacific region, I have, I suppose you might say, a different historical perspective.

When we look at the broad picture in terms of the Asia-Pacific region and its experience, transitioning is what I look at in the period of the last 60 or 70 years. The fact of the matter is when China first became independent in 1949, with over 400 million Chinese living at the time, and you look at the fact that here we are barely experiencing the fact that we are almost 300 million after establishing our own sense of democracy, less than 300 years, over the last 250 years, our population is less than 300 million. Now, the People's Republic of China has 1.3 billion people.

To me, regardless of how you label the kind of system of government that the Chinese leaders and the people have established thus far, the fact of the matter is I have to give them some sense of credit. How do you provide a system of government to feed 1.3 billion people out there, whether it is a democratic form or what? I would like to use the word "transitioning" probably as the best way that I could describe.

The fact of the matter, Mr. Chairman, is the Asia-Pacific region has gone through tremendous transitioning. Some of the dialogue that we have had in the times past in this Committee looking at the fact that colonialism was not a bad word 60 or 70 years ago, except for the most repressive administrations toward some of

these countries that we now find ourselves in the Asia-Pacific region: The French in Vietnam, the British in China, the Dutch in Indonesia, for some 350 years the most brutal colonial experiences that the Asia-Pacific countries have experienced.

I suppose one reason I ask sometimes my colleagues, why do you suppose a lot of these Asian leaders end up becoming Marxist socialists? That is because the worst examples of democracy are those supposedly exemplified by the western nations that extolled some principles of democracy during the period of colonialism who were out there carving empires did not paint a very pretty picture, in my humble opinion, in terms of the experiences that the Asia-Pacific have experienced at that period of time.

So there is one word that I would like to share with my colleagues. China is transitioning. Internet technology was introduced in China in the mid-1990s. According to the People's Republic of China data, the number of Internet users in China, not including Hong Kong, Macau, and Taiwan, reached over 111 million in 2005, making China the second-largest Internet population in the world. Internet usage is expected to rise as China continues to promote Internet development and enjoy rapid economic growth notwithstanding that the PRC Government strictly controls news and political content online, which has drawn the attention and criticism of many analysts and my colleagues here as policymakers from our country.

Frankly, I do want to commend China for controlling pornographic, violence-related, gambling, and other harmful information. At issue today is whether or not United States investment in China's Internet industry has led to the greater flow of global information in the country or whether or not United States corporations are overlooking violations of freedom of expression in China in order to maximize their profits.

Today, United States Internet companies in China reportedly are considering how to develop common responses that would attempt to strike a balance between promoting freedom of expression and operating within an authoritarian political system. Like former Secretaries of State James Baker and Madeleine Albright, I also believe that the growth of the Internet and other information technologies will help bring about wide-scale democratization abroad. As one from the Asia-Pacific region, I also believe the United States should be respectful of growing democracies, as I commend the U.S. corporations who are working to bring this about.

I believe it was Tom Friedman's recently written book, *The World Is Flat*, that presents an interesting observation about the scale on the globalization aspects of looking at information technology. It kind of had its beginning among nations then among the corporations. Now, it is with the individual. An individual in China can directly communicate with individuals here in America or any other part of the world.

It seems that with information and freedom of the press, we have some of our own problems. Why the *New York Times* was told for 1 whole year not to present its, I guess you might call, little leak about domestic surveillance because of our national security in place, which now raises a very interesting question about the right of the public to know whether or not the Administration can con-

duct domestic surveillance without having to get warrants from the Court.

A very interesting situation in our own country calling about freedom of expression and how we are having to go through this interesting debate about the Fourth Estate and its right to tell the public what is happening, causing at least this Member to raise issues in our own country when we talk about freedom of expression, why the *New York Times* took a whole year. Why did it prompt them all of a all of a sudden to say, well, I guess we had better tell them our sources, telling that there has been domestic surveillance these past 4 years by the Administration without having to get a warrant, a very interesting issue that we are debating in our own country about freedom of expression.

With that, Mr. Chairman, I want to just share that observation with my colleagues and look forward to hearing from our witnesses at the State Department as well as from our corporate community. Thank you, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. I thank my colleague.

The Chair recognizes Chairman Rohrabacher.

Mr. ROHRABACHER. Thank you, Chairman Smith, Chairman Leach, and Mr. Lantos, who again shows us that Republicans and Democrats share the ideals that are at the heart of our Government here in Washington, DC. Let me note if there is any question of transition going on and what direction transition is going.

What we are discussing today would indicate that China is in transition in the wrong direction, which is of utmost importance to the future of the United States and the stability of the world as well as to the people of China. Let me note that, yes, in a free society, when a free society is attacked, and a war is declared upon them by radical Islam, which we now face, certain things are permitted that would not be permitted otherwise. Yet this is no comparison to China, which is a government which is at war with its own people.

Corporate America, in dealing with these situations in the past, has a dismal human rights record. Now, whether it is Google or Yahoo! or any other, and we are not just picking on these particular high-tech companies, but any number of multibillion-dollar corporations who are doing business in China, they are carrying on this tradition of making a buck with no consideration for human rights or the American ideals that we supposedly all share. Again, we see a betrayal of America's ideals and an undercutting of those who are struggling for democracy and freedom in China. Not only, let me note, are China and the Chinese freedom of those people being undermined, but so are the long-term chances of peace between the United States and China and the stability of the world.

As I say, this is, again, a shameful act which we have seen so many times in corporate America, helping tyrants oppress their people, and now they do it again in an age of high technology, which shows us that technological development and sophistication of development, because we have been told all we need to do is help develop China's economy, and they are going to become more liberal, and here we see high technology and the development of industry in China is leading to more repression.

It is amazing to me that an American Internet company cannot connect the dots between profit and free and unfettered access to ideas. It is incomprehensible how they fail to see and to understand the implications to their own financial future by colluding with Chinese authorities to track down pro-democracy advocates or by setting up firewalls against such offending words as "independent judiciary" or "democracy." If and when China becomes a democracy, and those brave souls who are struggling now for freedom in these desperate circumstances in China, if they manage to overthrow their oppressor, these companies will be the first to be booted out by those who remember their betrayal and hypocrisy.

Today, we have in the audience an American citizen who happens to be a Falun Gong practitioner, Mr. Huan Lee. Before last week, he operated out of his home in Atlanta through his laptops communicating with people in China to help them get around the Internet firewalls that American companies have established. Well, he and other computer experts in Falun Gong have developed cutting-edge, antiblockage applications and technology of their own especially designed to help overcome these obstacles.

Well, last week, Mr. Lee, an American citizen, in his home in Atlanta, was attacked by Korean- and Chinese-speaking men. He was bound and tied and wrapped in a blanket and beaten. He needed stitches in his face. When I met him yesterday, his face was still black and blue. Then they asked in Chinese where his files were and took his computers, a hard disk, a cell phone, and his briefcase. Law enforcement authorities are investigating this attack, but at present the perpetrators remain at large.

Of course, in China, this would be common. What would be uncommon is that Mr. Lee would still be here. Mr. Lee, you are a hero of freedom. You are an American, and thus you are an American hero of freedom. I would ask you to stand for one moment. [Applause.]

Gentlemen—keep standing, Mr. Lee, for 1 minute—you have to choose between Mr. Lee and people like him in China who believe in our ideals as Americans and choosing between a gangster regime that beats people up and has heinous acts of oppression against their own people. It is your choice. Unfortunately, it appears that corporate America and you gentlemen have made the wrong decision. Thank you very much, Mr. Lee. [Applause.]

Mr. SMITH OF NEW JERSEY. Thank you very much, Dana.

The Chair recognizes Mr. Sherman.

Mr. SHERMAN. Thank you, Mr. Chairman. I think there are two issues here. One is the free flow of information and censorship where the Internet has been a tremendous positive, and I believe the involvement in U.S. high-tech companies has made it net a greater positive. However, it is up to these United States companies to inform their customers that not all of the world's sites are available on the Worldwide Web if you are in China. It should not be www. It is not worldwide Web; it is Chinese-censored Web. Second, we need to do everything possible in the United States to punch holes through the Chinese firewall to develop techniques, and I commend the Falun Gong and others who are doing that.

What concerns me even more is privacy, where a breach of privacy has led to the imprisonment of several democracy advocates.

At a minimum, United States companies need to inform their customers of the degree to which the Chinese Government may get private information. When I go to Google.com, I see the privacy policy. What is interesting about that policy is it says they may cooperate with a court order. They may cooperate with a criminal investigation.

I hope when I look at it again it says, a criminal investigation of a democracy, not that Yahoo! will turn over my e-mails, which would not be that interesting, or maybe the Chairman's, which would probably be more interesting, if that is part of the investigation of the Government of Sudan or China. Customers ought to know what the privacy policy is, and it is not enough to say criminal investigation because there is a difference between Beijing and Washington.

Second, the delete key has got to be a delete key so that when one of your customers deletes a document, it is gone from your system completely, unavailable to the Chinese Government or anyone else. I am particularly concerned about the participation or possible participation of U.S.-based employees in aiding oppressive governments, and that is why I would like to work with Members of this Committee, particularly Chairman Smith, on legislation that would prevent U.S.-based employees of any company that has confidential information, ISPs or banks or whomever, insurance companies, et cetera, prevent all U.S.-based employees from turning over confidential information to an oppressive government unless our Government certifies that that information is being requested pursuant to a legitimate criminal investigation of a nonpolitical crime.

A request from China or a court order from China directing Yahoo! or Google or anybody else to turn over information, or Bank of America, to turn over information to the Chinese Government should be ignored until you know that that is a legitimate criminal investigation and not an attempt to put a democracy advocate in prison.

Finally, if we are talking about privacy, I do need to comment about the privacy of Americans. Regardless of what this Administration is actually doing, its attorney general and our President himself are asserting that every chief executive of this country can, without a warrant, seize any information necessary to further the war on terrorism, wide open, any information, and I would hope that the companies represented today would tell us that Americans logging on to your domestic sites will have their privacy protected to the full extent of your privacy policies and will not be turned over to the U.S. Government in the absence of a court order.

Otherwise, while those in China may see their privacy violated in the most heinous ways, we here in the United States may also find that perhaps some future President asserting these very broad interpretations of the Constitution is reading our e-mail, and I would prefer that that not happen without a court order. I yield back.

Mr. SMITH OF NEW JERSEY. Thanks, Mr. Chairman. Mr. Fortenberry.

Mr. FORTENBERRY. Mr. Chairman, thank you for holding this very important hearing, and thank you to the many witnesses who will help us today probe this very grave issue of people versus prof-

its, of expression versus repression, of the rights of human persons versus the plans of the collective.

The companies represented here today have been pilloried in the press, and rightfully so, for abetting repression in China and, in one case, for cooperating with Chinese authorities, on the one hand, while stonewalling the U.S. Department of Justice on the other.

Mr. Chairman, this situation is not good. Now, with that said, I want to listen to all of our witnesses to understand how American multinational corporations are working to reconcile fundamental ethical standards with their efforts to observe foreign laws that violate American principles of justice.

American leadership and innovation have spurred the creation of the Internet. This remarkable technical breakthrough has since become synonymous with globalization, the Industrial Revolution of the late 20th century. Now globalization does carry the potential for progress to benefit human kind, but it also involves unprecedented challenges, including the one here today. U.S. companies operating around the world are required to abide by the local laws of the countries in which they operate just as foreign companies are required to abide by U.S. laws. However, the question before us is whether U.S. companies have a further obligation to the U.S. Constitution and the Bill of Rights when local laws overseas conflict with the basic principles upon which our laws are based.

The case of Shi Tao has focused worldwide attention and harsh criticism on United States Internet service providers operating in China. Let me say at the outset that it is my sincere hope that no U.S. executive would willingly and knowingly collude in the detention and jailing of journalists. Nevertheless, the damage has been done, and that damage is very serious in human terms.

I submit that it is valid to argue that more truthful and good information is better than less information, that our Internet companies, which are second to none, should be free to continue leading and empowering the free flow of information worldwide. It is also valid to argue that this free flow of information is like a rushing global torrent that will eventually burst any dam that is in its way.

Nevertheless, these arguments will ring hollow to Shi Tao and others like him, and during this hearing we cannot turn back the clock for Shi Tao, but after this hearing it is clear that we can no longer settle for business as usual.

Now, given the collective ingenuity available to the companies represented in this room, I cannot imagine the need to throw up our hands in despair or that we would dare to settle for dismissing personal liberty as a cost of doing business. So I look forward to a candid discussion on the issue of safeguards, export controls, and other possible mechanisms that we can employee to further limit jeopardy to the citizens of the world who seek a free exchange of information.

Mr. Chairman, again, thank you for bringing together such a knowledgeable group of witnesses to explore the important issue of corporate responsibility toward American fundamental principles of justice.

Mr. SMITH OF NEW JERSEY. Mr. Blumenauer?

Mr. BLUMENAUER. Thank you. I appreciate our Committee's leadership, Chairs, and Ranking Members for initiating this discussion and for the passion that has been clearly in evidence. This is a difficult set of issues, and I think we have already seen important and valuable soul searching done in a variety of sources, including some of the companies that will be visiting with us today.

But I think the companies themselves are more an indicator of a much larger set of issues and problems, and I hope we are sitting back listening to them and thinking about how the various companies in the information age walk the line in compliance with U.S. laws, the laws in the many countries around the world that they are operating, how we provide information, what impacts this has right here in this country, as has been referenced by a couple of my colleagues, on our own war on terrorism.

I fully believe that in China, in the long run, truth in information will transform that country, and with several Members of this Committee, when given the chance in direct conversation with Chinese leadership at the highest levels, have been unstinting in pushing back in terms of issues of access, of freedom, of being able to advance some of our democratic ideals. The question remains how best to do it, who plays what role, especially for the United States Government, and this is a mirror on our own behavior.

I think there are issues we could talk at some length about: Unlawful spying on U.S. citizens; the limits, the guidelines we are going to give to technology companies in terms of complying with laws, real or imagined. There is a lot to be explored, and they could tell us about difficulties in dealing with well-intended legislation that some of us have voted for that has turned into a nightmare and posed legal problems.

I also think this Congress has to be very careful about the signals that it sends. I am one who thinks that our telling the Palestinians right before the election who they were going to vote for might have just pushed Hamas over the top, and the Chinese Government, with some 4,000 years of history, has not always been amenable to being hit by a crowbar by the United States Congress. I think we have to be surgical and careful about what we do so that it is not counterproductive, but that is Congress.

We are going to hear from the Administration ultimately when we wind down our comments because they are practicing diplomacy, and they have got a lot going on, from Six-Party Talks—the list is endless in terms of the environment, the economy, and global security. And we need to take a step back and have a deep breath there.

I am hopeful that, apart from the politics and the diplomacy and the practice of business, that Congress does not overreact. I am open to suggestions for legislation, but a lot of what we did with knee-jerk reaction in the collapse of Enron and MCI produced some intemperate legislation with Sarbanes-Oxley that has been frozen in time. We would not have done it that way if we had done it in a thoughtful manner. Our dual-use-technology export controls have created a sort of bizarre regime where thoughtful, independent observers will suggest that, with the best of intentions, we have created problems not just for American business but actually might be undermining some of our security objectives, and it is a bureau-

cratic nightmare. It is frozen in time, and Congress is incapable, once it is there, of going back and thoughtfully looking at it and making adjustments that most rational people say ought to be made.

I commend the leadership for taking and shining a spotlight. I think just by having this hearing, important things are happening. I am open to how we strike that balance, how we work with the private sector, work with the Administration, work with governments around the world, but I hope that this is just the first step of a thoughtful, longer-term discussion so that we, at the end of the day, do something that achieves what all of us agree needs to happen, but too often Congress fails in the way that we initiate it.

I appreciate your courtesy, and I look forward to further proceedings of this hearing.

Mr. SMITH OF NEW JERSEY. Thank you. Chairman Burton?

Mr. BURTON. Thank you, Mr. Chairman. I want to thank you very much for holding this hearing. I am a little disappointed in some of my Democrat colleagues in trying to equate what is going on in China with the war against terror and how our President and our country is trying to stop additional terrorist attacks on this country by making sure we monitor what potential terrorists are doing here and abroad. But I know it is an election year, and I can understand them doing that. They would like to get the majority back, so I guess we just have to tolerate that.

Let me talk just a little bit about the issue at hand. President Hu, when he took office in 2004, indicating, and people were believing, that there was going to be an era of good feeling between the United States and China and that there was going to be less repression, and, according to what I have seen, it has been just the opposite. There is more hard-line activity over there. The golden shield, which is going to police the Internet over there ostensibly to deal with potential lawbreakers and people who might be a threat to law and order, is really just a tool to put innocent civilians in jail who criticize or who disagree with the regime.

It is a totalitarian, Communist approach that has been used in the past, but what bothers me about these American companies is I am sure that Microsoft and Google and Yahoo! were all watching television several years ago when young Chinese had a Statue of Liberty in Tiananmen Square, and young Chinese people were standing in front of tanks because they were fighting for liberty and freedom and all of the things that we enjoy. And they remember the thousands of young people that were thrown into gulags over there—10 million people are in the Communist gulags today, 10 million, and they were thrown into these Communist gulags and made to eat gruel and make things that we buy, ad infinitum.

We were all horrified by that. It was horrible, and the whole world criticized the Chinese Government for their repressive tactics and how they were crushing, literally with tanks, crushing people who only wanted freedom. That is what the President has been talking about, freedom and democracy, for some time. That is what we are all about. That is what John F. Kennedy was about. That is what we have been about since the beginning of our Republic: Freedom and democracy and human rights for human beings around the world. And here we are in the technology age, and some

of the most successful and effective companies that we have ever seen—the richest man in the world started Microsoft, and I really admire Bill Gates. I think it is fantastic that a man could acquire that kind of knowledge and that kind of wealth from being a great technology leader.

But now it is being used to repress people in the most repressive government in the world, and I just cannot understand why these companies who are making so much money cannot do it in a different way, not supporting a repressive regime that throws their people in jail simply because they disagree with them or crushes them with tanks.

So today, Mr. Chairman, when we talk to the people from these Internet companies and these major technology companies, I would like to ask them if there is anything being done to create countercensorship software because if they are making all of this money from the Chinese Government over there, maybe it would not be a bad idea to throw a few bones to the people who would continue to like to communicate in a free and effective way without the threat of being thrown into a gulag.

I would also like to ask, and I hope they will think about this when they testify, and I would like to have my whole statement inserted in the record, if I might, Mr. Chairman, but I would like for them, if they do not mind, telling us how much money they are making from their contracts with China. I think it would be interesting for the American people to know how much money they are making in helping repress the people who would like to have freedom of communication and have freedom in their country.

This is a very important issue. I am not sure that anything we are going to say today or do today is going to change a lot because everybody knows, in corporate America and around the world, the dollar is very important. I am a free-enterprise advocate. I am a conservative Republican, and I believe in free enterprise, but I also believe, with free enterprise comes responsibility, and I hope the leaders of these companies will take to heart what is being said here today.

We did not want you guys to come up here just to beat on you. That is not what we wanted you to come up here for. Hell, I want you to make a lot of money. I want you to be successful. That is the thing that makes America tick, that makes us the greatest economy in the world, but at the same time, there is a responsibility that must be realized as well.

We really need to do everything we can to bring about freedom, democracy, and human rights in this world, and I hope that these companies will take this to heart when they leave today and maybe try to do something in a little different direction to bring about a positive change. And I would like to know how much money you are making from these contracts over there, and I hope you will tell the American people. With that, Mr. Chairman, I yield back my time.

[The prepared statement of Mr. Burton follows:]

PREPARED STATEMENT OF THE HONORABLE DAN BURTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF INDIANA, AND CHAIRMAN, SUBCOMMITTEE ON THE WESTERN HEMISPHERE

MESSRS. CHAIRMEN, THANK YOU FOR HOLDING THIS IMPORTANT AND TIMELY HEARING. I LOOK FORWARD TO HEARING FROM OUR STATE DEPARTMENT OFFICIALS, PRIVATE SECTOR REPRESENTATIVES, AND THOSE REPRESENTING THE NON-GOVERNMENTAL ORGANIZATIONS AND HUMAN RIGHTS COMMUNITY.

WHILE I WHOLEHEARTEDLY BELIEVE IN A FREE ENTERPRISE SYSTEM AND THE SPIRIT OF CAPITALISM, I ALSO BELIEVE THAT WE MUST WORK TOGETHER TO FOSTER AND NURTURE DEMOCRATIC REFORM IN CHINA AS A CRITICALLY IMPORTANT STEP TO ENSURE THE LONG-TERM ECONOMIC AND SECURITY INTERESTS OF THE UNITED STATES.

IN RECENT YEARS, THE UNITED STATES CONGRESS HAS WORKED ON A BIPARTISAN AND BICAMERAL LEVEL TO SEND A STRONG, CONSISTENT MESSAGE TO REPRESSIVE REGIMES LIKE THE PEOPLE'S REPUBLIC OF CHINA (PRC): OPEN THE FLOODGATES AND MAKE A REAL COMMITMENT TO SUPPORT AND ADVANCE DEMOCRATIC GOVERNANCE AND POLITICAL OPENNESS, RESPECT HUMAN RIGHTS, AND PROMOTE AND PROTECT FREEDOM OF SPEECH.

WE MUST WORK TO ENSURE THAT U.S. COMPANIES WHICH ACTIVELY PARTICIPATE IN BUSINESS CONTRACTS WITH THE PRC DO SO IN A TRANSPARENT AND LEGITIMATE MANNER. TO THAT END, WHILE I REMAIN GREATLY CONCERNED ABOUT THE PRC'S OPPRESSIVE TACTICS, I WAS ALSO TROUBLED TO HEAR THE LATEST DEVELOPMENTS SURROUNDING THE DISCOVERY THAT AMERICAN COMPANIES ARE ALLEGEDLY COMPLICIT IN SUPPORTING CHINA'S REPRESSIVE ACTIONS.

EVEN THOUGH THE ARRIVAL OF THE CHINESE INTERNET IN THE MID-1990S PROVIDED THE AVERAGE CHINESE CITIZEN WITH THE ABILITY TO MORE RAPIDLY EXCHANGE IDEAS, IT ALSO BROUGHT ABOUT THE DEBILITATING USE OF STRICT CENSORSHIP AND THE LIMITATION OF FREE SPEECH. OVER 111 MILLION PEOPLE IN CHINA HAVE ACCESS TO THE INTERNET, AN INCREASE OF 88% IN JUST THE LAST THREE YEARS. IN FACT, THE CHINESE INTERNET IS THE SECOND LARGEST INTERNET MARKET BEHIND THE UNITED STATES.

SO, WE MUST ASK OURSELVES THE QUESTION: SHOULD WE REMOVE U.S. COMPANIES FROM CHINA AND HAND OVER COMPLETE INTERNET CONTROL AND DOMINATION—AND SUBSEQUENTLY, COMPLETE CENSORSHIP—TO THE CHINESE GOVERNMENT?

THERE IS A BETTER WAY; IT IS MY HOPE THAT USERS OF THE INTERNET IN CHINA WILL CHISEL AWAY AT THE VIRTUAL WALLS OF REPRESSION AND DEMAND THAT THE GOVERNMENT CEASE FROM CENSORING INFORMATION.

AS YOU KNOW, THE CHINESE GOVERNMENT OWNS ALL THE TELEVISION AND RADIO STATIONS IN CHINA, AND MOST PRINT MEDIA OUTLETS, SO AS TO PROPAGATE AND PROMOTE STATE-SANCTIONED IDEOLOGY AND INFORMATION.

MEDIA PROFESSIONALS OPERATE UNDER STRICT ORDERS TO FOLLOW CENTRAL PARTY DIRECTIVES AND TO 'GUIDE PUBLIC OPINION' AS DIRECTED BY POLITICAL AUTHORITIES WHO EVEN GO SO FAR AS TO DIRECTLY CENSOR BOTH THE DOMESTIC AND FOREIGN MEDIA TO ENSURE COMPLIANCE.

NOW, THE HEAVY HAND OF CHINESE CENSORSHIP EXTENDS INTO THE UNTAMED ELECTRONIC WILDERNESS THAT IS THE INTERNET. AS I UNDERSTAND IT, THE OFFICIAL PRC PARTY LINE IS TO PROMOTE THE USE OF THE INTERNET, WHILE IN REALITY HEAVILY REGULATING AND MONITORING ITS USERS.

ACCORDING TO THE STATE DEPARTMENT'S ESTIMATES, CHINA'S INTERNET CONTROL SYSTEM EMPLOYS MORE THAN 30,000 PEOPLE—THROUGH AN OFFICIAL BUREAUCRACY—TO SPECIFICALLY TARGET AND PUNISH INTERNET USERS WHO QUESTION, CRITICIZE, OR STRAY FROM THE ACCEPTED, HEAVILY-CENSORED LANDSCAPE OF TOPICS AND COMMUNIST PARTY DOGMA. IN OTHER WORDS, CHINESE CITIZENS USE THE INTERNET AT THE GREAT RISK OF PUNISHMENT AND IMPRISONMENT—MORE SO THAN EVEN CONVENTIONAL MEDIA.

IT HAS ALSO BEEN BROUGHT TO MY ATTENTION THAT THE PRC'S MINISTRY OF PUBLIC SECURITY HAS BEEN CONTINUALLY UPGRADING AND

EXPANDING ITS "GOLDEN SHIELD" PROJECT—A GOVERNMENT-SPONSORED SURVEILLANCE SYSTEM THAT WAS INAUGURATED IN 1998.

THE GOLDEN SHIELD PROJECT INCLUDED THE CONSTRUCTION OF AN ADVANCED COMMUNICATION NETWORK AND COMPUTER-BASED INFORMATION SYSTEM PURPORTEDLY TO BE USED TO IMPROVE POLICE EFFECTIVENESS AND EFFICIENCY. UNFORTUNATELY, AS WE HAVE DISCOVERED, THE PRC IS NOT USING GOLDEN SHIELD AS A TOOL TO IMPROVE POLICE EFFICIENCY, BUT AS A WAY TO MONITOR CHINESE CIVILIANS VIA REMOTE VIDEO SURVEILLANCE, ONLINE DATABASES CONTAINING IDENTIFICATION RECORDS OF CHINESE CITIZENS, AND INTERNET POLICING.

WE MUST NOT OVERLOOK THESE EGREGIOUS VIOLATIONS OF FREEDOM OF EXPRESSION IN CHINA. WHILE THE INTERNET HAS PLAYED A ROLE IN BRINGING GLOBAL ATTENTION TO THE ISSUE OF CHINESE CENSORSHIP, THE INTERNATIONAL COMMUNITY MUST DO ALL THAT WE CAN TO ACTIVELY PROMOTE THE FREE FLOWING EXCHANGE OF IDEAS THROUGHOUT THE REPRESSIVE REGIME.

A STEP IN THE RIGHT DIRECTION WOULD BE TO PROMOTE THE DISTRIBUTION AND USAGE OF COUNTER-CENSORSHIP SOFTWARE.

IN FACT, I AM A PROUD COSPONSOR OF REPRESENTATIVE COX'S "GLOBAL INTERNET FREEDOM ACT OF 2005" (H.R. 2216), WHICH WOULD AUTHORIZE $50 MILLION TO DEVELOP AND IMPLEMENT A GLOBAL INTERNET FREEDOM POLICY COMBAT STATE-SPONSORED AND STATE-DIRECTED INTERNET JAMMING BY REPRESSIVE FOREIGN GOVERNMENTS—SUCH AS THE PRC—AND THE INTIMIDATION AND PERSECUTION BY SUCH GOVERNMENTS OF THEIR CITIZENS WHO USE THE INTERNET.

IN THE SAME VEIN, SINCE HE ASSUMED POWER IN 2004, PRESIDENT HU JINTAO HAS DISAPPOINTED THOSE OF US WHO EXPECTED DEEPER AND MORE MEANINGFUL OPENING OF CHINESE SOCIETY. PRESIDENT HU HAS TAKEN A HARDER LINE TO SUPPRESS FREEDOM OF PRESS AND RELIGION, WHILE STOKING CHINESE NATIONALISM WITH THE ULTIMATE RESULT OF REPRESSION AND XENOPHOBIA. THERE IS A DARK SIDE OF NATIONALISM AND PRESIDENT HU HAS DEMONSTRATED A TENDENCY TO USE NATIONALISM AS A JUSTIFICATION FOR AUTHORITARIANISM.

WHILE TODAY WE ARE LOOKING AT INTERNET USAGE AND CONTROL OF THE INFORMATION SUPERHIGHWAY WITHIN CHINA, I WANT TO ALSO REMIND MY COLLEAGUES THAT CHINESE MILITARY STRATEGISTS HAVE ADVOCATED EXTENSIVE HACKING AND THE INTRODUCTION OF COMPUTER SUPER-VIRUSES AS METHODS TO "GAIN DECISIVE EDGES OVER ADVERSARIES."

AS WE ALL KNOW, CHINA POSSESSES A BOOMING HI-TECH INDUSTRY AND I AM CLOSELY WATCHING TO SEE WHETHER THERE IS A POLITICAL WILL AND COMMITMENT TO USE THESE TECHNOLOGIES FOR PEACEFUL MEANS WITHIN AND BEYOND CHINA'S BORDERS.

MOREOVER, CHINA WILL HOST THE OLYMPIC GAMES IN 2008, AND THERE MUST BE SUSTAINED INTERNATIONAL PRESSURE ON CHINA TO BREAK FROM THE PAST TO PURSUE AND INSTITUTIONALIZE DEMOCRATIC FREEDOMS AND INSTITUTIONS.

MESSRS. CHAIRMAN, THANK YOU FOR HOLDING THIS VITALLY IMPORTANT HEARING. I LOOK FORWARD TO HEARING FROM THE COMMITTEE'S WITNESSES AND FINDING A VIABLE SOLUTION TO ADDRESS THE GROWING PROBLEM OF CENSORSHIP THROUGHOUT CHINA.

Mr. SMITH OF NEW JERSEY. The Chair recognizes the gentlelady from California, Ms. Watson.

Ms. WATSON. Thank you, Mr. Chairman. I am very pleased that you are holding these important hearings on the role of the Internet in China. Let me try to be as brief as I can.

Certainly, no Member likes the fact that United States-based Internet gateway companies, such as Yahoo! and Microsoft, have been implicated in providing information to Chinese authorities that has landed its clients in jail. Neither are Members pleased about the reports that United States companies have cooperated in filtering their sites of political content the Chinese Government finds objectionable and provided technology to enhance the capabilities of Chinese censors to monitor the Internet. The actions rub

at the fundamental principles of an open society which cherishes and thrives on the free exchange of ideas and information.

Despite the PRC's efforts at censorship of the Internet and their odious consequences, we also must not forget that the Internet is an incredible force for freedom and change around the world. It is my understanding that China now has somewhere around 166 million e-mail accounts. Those with access to computers conduct nearly 400 million Internet searches daily. A significant amount of this activity escapes Chinese censors' eyes. For example, it is my understanding that much of the information about growing discontent in the provinces is communicated throughout China via the Internet. The Chinese Government's attempt to put a lid on the outbreak of SARS was undermined by Internet communication.

Mr. Chairman, it is my hope that this hearing will become part of a constructive dialogue about the challenges to Internet freedom and perhaps lead down the road to a responsible and standardized set of industry practices that all U.S. Internet companies will follow.

I also believe it is proper and very timely that Secretary of State Condoleezza Rice announced yesterday the formation of a new, global, Internet freedom task force that will attempt to address the challenges of Internet freedom. I would be interested in hearing the Administration's thought on the new task force.

Finally, Mr. Chairman, I want to note the absence of China's largest search engine company, Baidu, which you may have invited to the hearing today. Baidu controls more than 50 percent of the Chinese Internet search market. It is listed on Nasdaq, has American investors, and has voluntary submitted to Chinese censorship. I believe that it would have been very enlightening to have their representatives at the witness table today, so I hope at another time they will come and testify in front of this Committee. Thank you very much, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. Thank you very much.

Mr. Tancredo?

Mr. TANCREDO. Mr. Chairman, as several times in the past I had originally chosen not to speak at this time because we are here gathered to hear the testimony of the people that we have brought into the room, but, once again, some of the comments of my friends on the other side force me to interject my own thoughts on this. And that is that this Committee and our Human Rights Caucus have held several hearings on the issue of torture, and I sometimes think, in listening to my colleagues on the other side, that they could be brought in front of that committee for the torture they do to logic, especially when they try to draw comparisons, these bizarre and outlandish and idiotic comparisons, between colonialism and the fact that there is an attempt on the part of our Government to identify people who are talking to our enemies, that is to say, identify people who are communicating with al-Qaeda, and somehow make that a relative act, relatively the same.

What the heck? Whether or not China, a country with a human rights record that should be and is often condemned by most of the civilized world, a country that does what it does to its own people, a country that has no regard for human rights, that in any way these two actions, the actions taken by the government to try to

get these Internet operators and high-tech providers to give them the information they need to imprison people who are talking about things like freedom, it is just ridiculous to try to make these comparisons and to try to make the world feel as though these actions are in any way, ours and theirs, similar. They are not.

We are operating two different systems where what we are doing today could never be done, of course, in China. Looking into these issues is not allowed. The ability for us to analyze our own problems and to share them with the world, which we do so regularly; that certainly never can be done in China.

It is interesting in a way to me because in the original discussion of PNTR, permanent normal trade relations with China, we had so many companies coming in to tell us that, in fact, if we only would give them the ability to trade with China and to do so on a preferred basis that all of a sudden Jeffersonian democracy would break out all over China as a result of this economic vitality that we would create.

I remember saying at the time, if that were the case, why would the Chinese be here lobbying for this? Who knows more about China, us or the Chinese? The fact is that they wanted PNTR. They wanted it because, of course, a more vibrant economy helped them control their population. It helped them solidify their position. They do not want this freedom, however. They do not want the freedom of the Internet for exactly the opposite reason, because it would destabilize the regime, and we should, of course, understand what motivates, and we should do whatever we can to expand that concept of freedom throughout the world, and one way to do it is to let people have access to the free marketplace of ideas.

We should not be fearful of the free marketplace of ideas. There will be some we do not like listening to, but it is nonetheless good for us to be able to explore them, and it is good for the Chinese people to be able to explore them. It is a healthier world we would create, and it is a less dangerous world we will create if that kind of opportunity is afforded to all people in China. Thank you, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. Thank you.

Ms. McCollum?

Ms. MCCOLLUM. Thank you, Mr. Chair. I was hesitant to speak because we have so many people waiting to listen to what we are going to hear from our Government, from the testifiers who have their opinions on what should be done, and then from the companies who are directly involved in this. But to say nothing when my friends, and I do regard some on the other side of the aisle my friends, when we, as Democrats, say we need to look at laws, we need to look at the laws which China has and which these corporations, which we have encouraged to go to China through trade agreements passed by this country, have to work within the rule of law of China.

I think having a discussion about what we do to promote our democratic values here at home and abroad is a legitimate discussion. I think having a discussion with these companies about what we can do to protect people in China as they access the Internet—I think privacy statements have been discussed. Maybe what should be showing up in a privacy statement is: "This site has been

filtered. It has been restricted by your government," or, "Your government may be monitoring this over our objections, over our company's values, but this is the arena in which we have to work in."

But then when some of my colleagues have talked about we, too, have to be ever vigilant to uphold the goals, the ideas, and the values of our United States Constitution and to make sure that we are participating in the checks and balances that are important in our democracy to remain healthy. For people to say that they are going to tolerate us saying that up here while people all around the world are watching does not speak well of us working together in a bipartisan way to do exactly what Mr. Tancredo said, to listen to one another, to learn from one another, and to have open and honest exchanges in which we are truly listening to one another.

To make comments that by wondering when we are going to have oversight hearings to find out how the Executive Branch is using its gathering of information through the Internet and through other technologies to listen in on what American citizens may be doing or may not be doing is somehow unpatriotic and that somehow, as a mother and as a person who took an oath of office to defend this Constitution, I am not a true American is wrong.

So what we need to do here today is to listen to the challenges that are out there for corporations as they interact with governments such as China in having their customers access the Internet and work with them to create an open society on the Internet. What we also need to do is to do our job here at home in our obligation to make sure that checks and balances are fulfilled so that we, at the same time, are looking clearly and making sure Americans' privacy rights are protected. Thank you, Mr. Chair.

Mr. SMITH OF NEW JERSEY. Thank you very much.

Chairman Royce?

Mr. ROYCE. Yes. I do not think anyone, Mr. Chairman, is making the argument that no one is a true American because they might suggest a moral equivalency argument. All we are saying is that, or I think the point my colleague is trying to make is that, before 9/11 the NSA was eavesdropping, and we might as well admit it, on al-Qaeda on the pilots potentially who were going to take a plane and crash it into the Pentagon. Now, there were about a dozen calls that came out of Yemen where we listened in.

Now, the NSA was concerned enough about civil liberties that they knew that these two al-Qaeda agents were now in the United States, and thus to be treated like citizens, they did not set up their electronic equipment on this side, in the United States, and did not follow the conversations in the United States.

What subsequently happened, just by way of explanation, is that in the United States the NSA, under orders from the President of the United States, decided that in the future if, through the al-Qaeda switchboard in Yemen or anywhere else in the world, al-Qaeda attempted to make contact with their agents in the United States, we would, in fact, follow up in the U.S. instead of making this an area where those agents might operate without oversight, and we did that because, in addition to this particular incident, we had several other incidents that we were able to prevent on United States soil and in Europe through the use of this technology.

Arguably, for those of us on this side, this does not seem to be the same moral equivalency argument that we are involved in vis-a-vis the whole discussion of China. I think the thing that troubles us about those companies that have gone above and beyond the censorship that China demands of them as a cost of doing business, and we certainly have listened to the argument of the companies, they say that their issue is offer censored Internet service or offer none at all.

We understand that argument, but what I think gives us particular pause right now and drives this hearing is that Yahoo! provided evidence to Chinese authorities that led to the imprisonment of Internet writer and activist Li Zhi, and the difference between imprisoning or monitoring and affecting his conversation as opposed to an al-Qaeda agent is demonstrably different because what you are talking about here is someone who is simply trying to articulate the position that freedom of speech is an important right in China, and part of Chinese evolution is accepting a divergence of opinion.

The cooperation of Yahoo! with the Chinese police led to his arrest and subsequent 8 years' prison sentence. It is one thing to play by another country's censorship rules, as odious as they may be, as is the case here, but it is a very different matter to aid in ruthless persecution of free thinkers, and for those of us that want to protect the environment for free thinkers in the world, I think it is important also to delineate the difference between someone involved in freedom of expression and someone involved in terrorist activity.

I, by way of my meager effort to offer a partial solution to this that I think might help compensate in some way for the damage done, would make the following observation. Some of the best minds in the world are involved in developing this new technology, and it strikes me that those same minds could be involved in developing ways to break through jamming.

For many years, I have carried legislation including Radio Free Asia. I have expanded the broadcasting now. We built the largest and most powerful transmitter in the world on Tinian Island with legislation I have carried. One of the things that really frustrated me about United States industry, and I will be very blunt about this, after we developed that capability, allegedly a company in Texas then went to the Chinese authorities and offered them the technology to jam Radio Free Asia in order to silence the ability to disseminate information across Asia.

Now, what steps might industry take now? How could we find a way that could repair some of the damage? I would suggest at least the consideration of an idea, and I would prefer this outside of the government. I am not a big enthusiast for government involvement unless it is to set up something like surrogate radio service in some place in the world where there is no functioning free speech. I can see the utility in that, but I prefer the private market.

So my suggestion might be that those involved in an interest in free speech, because there is a great commitment to that with respect to many of the people that are going to appear here today, or at least in the past they have articulated that position, consider setting up some kind of a fund, privately maintained, that will help fund and consider contributions in technology that will help over-

come the jamming, that will find ways around the censor of the Internet, and make that available.

I would think that that would be something that would maybe even offset the reputation that some United States companies have created, like the one I cited in Texas that allegedly then sold to the Chinese Government the very technology that would allow them to jam. They had been a part of helping to develop it. Our taxpayers paid for a United States company to help. It was part of the effort to develop the broadcasting capabilities, and then they turned right around and sold that to the Chinese Government.

I do think that there is, in the interest of freedom, a stakehold in this for many of the personalities in this room today, and I think their minds should be focused on what the private sector can do to help, as I said, overcompensate for some of the damage done.

Chairman Smith and others have spoken eloquently about China's abhorrent human rights record. They are right. We, as a country, owe it to ourselves to look as closely as we can at these difficult issues which will profoundly impact the Chinese people's future and, frankly, long term, will impact our own nation's well-being. Thank you very much, Chairman Smith.

Mr. SMITH OF NEW JERSEY. Mr. Meeks?

Mr. MEEKS. Thank you, Mr. Chairman. I have been listening. Let me first start by this because I think that, first, in the spirit of honesty and in the spirit of truth, for me as I listened to my colleagues on the other side talking about whether or not this is equated to the NSA, et cetera, let me just say, in the spirit of Black History Month, first of all, many blacks in this country, when we had the founding fathers, they did not have freedom. In fact, for over 200 years, there was no freedom. We just lost Coretta Scott King. What they were fighting about as recent as a few months ago is freedom, and we have got to practice what we preach.

Freedom has not been for everybody here in America. Just ask some of the individuals in New Orleans. So we have got to make sure sometimes that we practice what we preach and that we do not try to blame someone else for some of our own failings.

Freedom is work, freedom is sacrifice, and freedom is making a difference. Now, for me, freedom is not just pointing fingers at American companies whom we said, and I know some way, well, the Chinese wanted them—well, we said we wanted them to be in China. Why? Well, I know I voted for PNTR. Why? Because I think that most of our American corporations and American businesses doing business in China have been some of our greatest Ambassadors. I think sometimes we forget the fact that China has changed substantially over the last 20 to 25 years, and it is, I think, a direct result of many of our businesses that are doing business in China.

I was told one thing prior to visiting China, but going to China, I was told before I left that if I would talk to any Chinese individuals on the street, that they were so fearful of their government, they would not talk to me. They would run from me for fear of being locked up and put in jail. Well, I wanted to test that theory myself because I know that that would have happened some 20 to 25 years ago.

I got an interpreter and a car, and I stopped at bus stops that no one could have possibly known that I was going to stop at just to see what the reaction of the Chinese people would be and to ask them what their reactions were and what their feelings were toward the American companies doing business in China. I was quite shocked. It was not what I was told before I left.

I found that the Chinese people were very engaging and very appreciative of our American businesses. In fact, most of them desired to work for the American businesses because they saw it as a road to a better life and to freedom. We had some great off-the-record conversations. So for us to now come and say that because our American corporations are abiding to the laws of China that they are at fault, I think not.

I think of all of the communications that were completely cut off in this country. Long before the NSA, there were wire taps and other illegal activity that took place with Dr. King. Long before that, there were people that were jailed, one, a Member of this Congress, a member of the Black Panther Party. I am sure he can go into a whole lot of things that took place with reference to that organization.

But we have got to continue to push and pursue freedom but not say we are going to, number one, point fingers at our companies. Maybe here is a role and an opportunity for the State Department and the International Society to get together so we can set some rules for all companies, no matter where we have Internet access, as opposed to saying that now something that we all voted for, or most of us in this Congress, for PNTR, to say, now we are going to point a finger at you, company, or that company. I do not think that is the way to go. It is right to compare what we do in this country to what other countries do.

So to say to us on this side that we should not be, well, it is not only for me, not only about NSA. It is about the historical background of all kinds of other kinds of illegal activities that this Government, Democrat or Republican, have taken place, and people have had an effect when they were just trying to fight for freedom. But we did not stop and listen to our local newspapers or anyone else who said it was prohibited, that we are not going to allow you to continue to do business there.

So I say that we need to work at this thing collectively. We need to make sure that we are working together so that freedom for the Chinese people can come, but do not put ourselves in the position where individuals are looking at us and making us the laughingstock because, again, we are saying do something, and then we are not doing it ourselves.

We have got to make sure that not only we tell people what to do and how to do it, that, in fact, we lead the way by doing it ourselves, and that is what this is all about. This should not be about just pointing fingers at our American companies, who I believe have been great Ambassadors and have forwarded more peace, more freedom, I should say, and more opportunity to the people of China, and as long as that information continues to flow, you cannot stop it because truth will continue to roll like the waters around the globe. I yield back.

Mr. SMITH OF NEW JERSEY. Adam Smith?

Mr. SMITH OF WASHINGTON. Thank you, Mr. Chairman. I appreciate the opportunity to speak, and I appreciate you having this hearing. I think this is an incredibly important discussion. When you are talking about interacting with regimes that you disagree with, there are a lot of very complicated and important issues that come up, and certainly this is not limited to China, and it is not limited to private companies. State-to-state issues arise as well, and I just feel that it is not a black-and-white issue. It is not engagement always works. No matter how bad they are, no matter what they are doing, simply engage, and it will get better. Nor is it true that simply saying, Look, if we disagree with you, we are going to have absolutely nothing to do with you. I do not think that is a smart approach either.

I think you have got to look at it on a case-by-case basis, and where China is concerned, it is particularly important because we are talking about 1.4 billion people and the most prominent emerging power in the world. Having a positive relationship with China, I think, is incredibly important to the future peace and stability of the globe.

When we look at this particular issue, the one thing that occurs to me is, let us assume for the moment that no United States tech company does business in China. Does it get better? Is it less repressive? Does China move forward? I do not think so, not in the least bit. I think lashing out at the companies there as sort of enabling this is a little absurd. China is what China is, and if the tech companies leave, that is not going to change.

So we have to look at what are we doing, and is it going to make a positive difference? I think one of the positive differences that is out there is what Mr. Meeks referenced, and this is what I am hearing from countless sources. While there is no question that China is a repressive regime, and you can pick your example and bash on it in a number of different ways, I think the question is, is it getting any better? The story I am hearing is that it is, that, in fact, there is greater freedom and openness amongst the people than there was 5, 10, 15, 20 years ago.

So if we are making progress, that is something to make note of. It is not standing up and saying it is all perfect, it is all beautiful, and I do not remember anybody promising Jeffersonian democracy the year after we passed PNTR, by the way. I think there was a far more realistic approach, that you engage, and you make progress, and you move forward.

We do not have the power, as big and powerful and strong as we are as a country, to simply point around the globe, and I would trust this lesson would be learned quite clear by now, snap our fingers and say, You will do this the way we want you to. It is more complicated than that, but I think we are making progress in China.

When you talk about the Internet, in particular, I think the most interesting aspect of this, yes, they require filters. Well, we require filters around here. Private companies require filters as well, and yet I think we would all know that those things are only so effective. They are consistently broken, consistently hacked into, and the same is happening in China. China is not going to be any more successful at filtering and firewalling everything than we are. If

you have it there, people will get through those firewalls and get information that they otherwise would not, and that is undeniably happening right now. So I think we have to be mindful of that.

Now, one thing I will say is that we have some leverage here, and I hope that our companies, and I think our role on this Committee is to put pressure on our companies that are over there doing business to use that leverage as well as they can. I think we must be realistic about that in negotiating with China to try to make progress and move forward, but I think it would be a grave mistake for this Committee to stand up and say, Look, China, we do not like what you are doing. Therefore, we just do not want to talk to you or have anything to do with you. I think progress is being made. I think the Internet is one way to do that.

I do think we sometimes get a little pie in the sky about the progress that is going to be made, that it is going to be instantaneous and comprehensive. It is not going to happen. It is going to be slow and steady, and I think it is.

So while I look forward to this discussion, and I want to hear more about what is going on over there and how we can help move the ball forward to make the regime less repressive and more open, I do not think the approach here is to simply bash on the companies for doing business with China. It is far, far, far more complicated than that. Progress is being made. I hope we can work with the companies and with our own State Department to figure out how to make more progress but not to create a new Cold War with China by saying, "We disagree with you; therefore, we will never have anything to do with you." I think that would be a very grave mistake for our foreign policy, so thank you for the opportunity.

Mr. SMITH OF NEW JERSEY. Ranking Member Payne.

Mr. PAYNE. Thank you very much, Mr. Chairman. Thank you for calling this very important and timely hearing. I do not know of any issue more prominent as relates to relationships between the U.S. and the PRC than this issue right now.

More than 100 million people in China are Internet users. China has become the second-largest country of Internet usage in the world ever since the Internet was introduced there in the 1990s. Because of the huge population, estimated between 1.3 and 1.5 billion people, and rapid economic growth, the number of users is increasing very fast, spreading from the metropolitan cities in the eastern areas to the cities and even small towns in middle and western regions of the country. It is spreading like wildfire.

The Internet has been shaping Chinese society and changing the way of ordinary people's lives throughout that nation. However, politically, the Internet is both a tool for freedom and repression. It is sort of a tale of two cities: The best of times and the worst of times. The fact is that at the beginning the West was generally optimistic about the role the Internet would play in China. They said the Internet would accelerate liberalization and freedom of speech.

The assumption was that the Internet is impossible to control and censor. Former President Clinton once said that trying to control the Internet would be like trying to nail Jello to the wall. Unfortunately, and if anybody could do it, he probably could have done it, unfortunately, the Chinese Government has managed to do

that, and United States companies have been involved. That is why we are here today at this hearing.

I think it has been mentioned that if we had been a little less anxious to change what was called Most Favored Nation status, which China enjoyed, but it was a trade treaty that had to be approved on a regular basis. There were people who felt that, first of all, the name sounded too good because the jury was still out on the People's Republic of China, and to have something called the Most Favored Nation status for trade relations sounded too good, and so those people who think of names that are very positive—the most positive a name sounds, the more suspicious I get. But then Most Favored Nation status, as we all know, was changed to permanent normal trade relations.

PNTR. That sounded a little less cozy, a little less favorable, especially in light of Tiananmen Square, in spite of the imprisonment of religious leaders and so forth. So we now have permanent normal trade relations, which means that we cannot reopen this unless it is some dramatic act of Congress that can undo a trade law, which would be almost impossible at this time. Why it was felt that we should give away a tool to keep a country that was emerging out of total totalitarianism into attempting to have some kind of democracy and free enterprise, to me, made no sense at all.

The Chinese Government requires all companies to comply with its regulations on censorship and control of information. Companies like Yahoo!, Google, and Microsoft have complied, which we would expect them to do if they are going to do business in the PRC.

I am very concerned and disturbed by the actions of Yahoo! disclosing the e-mail addresses and contents of cyber-dissident Li Zhi and Shi Tao to the government, respectively, in 2003 and 2004, which has already been mentioned, resulting in Mr. Lee's 8-year sentence and Mr. Shi's 10-year sentence.

In 2004, Cisco Systems and Juniper Networks were involved in assisting China to develop censorship capabilities in trading for four out of the six contracts from the Chinese Government. Microsoft's blog-hosting service, MSN, at Beijing's request, closed down the popular online journal of blogger Zhao Jing, who also worked as a research assistant in the Beijing bureau of the *New York Times*.

In 2006, the new local Google site in China, www.google.cn, will comply with local Chinese laws and regulations, move the key words like "democracy" and "human rights," "Tibetan independent," "Tiananmen crackdown," "Falun Gong spiritual movement," "Taiwanese independence" from use in the Chinese search engine. That is total censorship. It is absolutely wrong.

All of these facts are disturbing. These companies must find ways to work around this brutal censorship whenever possible, but I am afraid that if these companies were asked to leave China, the Chinese people would be the ones to suffer. You mentioned before, Glasnost and Perastroika in the USSR was a gradual, time-consuming, year-in-and-year-out by virtue of contact between western people, youth groups visiting the people in the USSR finally saw the breakdown of that system of the Warsaw Pact countries, and the wall came down in Berlin.

It was a slow process. With the Internet, these things can be accelerated. However, as I have indicated, it can also be the worst of times, as it could be in the best times. So 10 years ago, no one would have imagined we would be talking about Chinese end users on e-mail and Web blogs, but today the activities of ordinary Chinese citizens on these Internet services flourish.

So though censorship is wrong and should not be used, it is a reality in China right now, and these companies have to operate in that reality. I think it is more useful for the United States companies to be operating in China and providing access to information and outlets for cultural expression and opinion sharing than for Chinese people to have to rely on Chinese Internet providers which do self-censorship and even blog more information.

We also have to remember that most Chinese citizens who use the Internet are not going to look for information on Falun Gong or Taiwanese independence anymore. In other words, the Internet is much more than a tool for political use, and our attempt to reduce the issues to that could have unintended consequences.

Once again, as I voted against the Most Favored Nation status or permanent trade relations, I think if we still had it open, we could pressure China, for example, even in Darfur where they are extracting the oil or looking the other way as genocide is going on, and they, being a permanent member of the Security Council, can veto any strong resolution condemning what is happening in Darfur. That is the reason that the Secretary-General's hands are almost tied, because of the Security Council and those five permanent members who can veto any proposal. We have no real clout over the head of the Chinese Government.

So, Mr. Chairman, I really commend you for this hearing. I certainly look forward to hearing testimony from our witnesses.

Mr. SMITH OF NEW JERSEY. Mr. Payne, thank you so very much.

Let me now introduce our first panel, panel 1, beginning with Ambassador David Gross, who has served since August 2001 as the U.S. Coordinator for International Communications and Information Policy in the Bureau of Economic and Business Affairs. Since joining the Department of State, Ambassador Gross has addressed the UN General Assembly and has led U.S. delegations to many major international telecommunications conferences. He has also led the U.S. Government's participation in the multilateral preparatory work for both phases of the UN's "Heads of State" World Summit on the Information Society and had the honor of leading the U.S. delegations to both the formal summit in Geneva in 2003 and in Tunis in 2005.

We then will hear from Mr. James Keith, who is the senior advisor on China, Mongolia, Taiwan, Hong Kong, and Macau at the U.S. Department of State. Prior to becoming senior advisor, Mr. Keith was consul general of the United States in Hong Kong and was the director of the Office of Chinese Affairs. Mr. Keith is a career foreign service officer. He has served numerous tours of duty in Washington working on Asian affairs and has served at the United States Embassies in Beijing, Jakarta, and Seoul.

At this time, if I could ask both of you two gentlemen to please stand and take the oath, and if you could raise your right hands.

[Witnesses sworn.]

Mr. SMITH OF NEW JERSEY. Let the record show that each of our witnesses affirmed in the affirmative, and, Ambassador Gross, the floor is yours.

TESTIMONY OF THE HONORABLE DAVID A. GROSS, DEPUTY ASSISTANT SECRETARY FOR INTERNATIONAL COMMUNICATIONS AND INFORMATION POLICY, BUREAU OF ECONOMIC AND BUSINESS AFFAIRS, U.S. DEPARTMENT OF STATE

Mr. GROSS. Thank you very much, Mr. Chairman. Should I ask for our written statements to be incorporated into the record?

Mr. SMITH OF NEW JERSEY. Without objection, both of your written statements and any attachments will be made a part of the record.

Mr. GROSS. Thank you very much, Mr. Chairman. Thank you, Chairman, and Ranking Members very much. I want to thank you especially for holding this hearing. As I think everyone has said this morning, this hearing and the holding of this hearing itself is a significant event and something for which we are already seeing positive changes.

Since its commercial launch a little over a decade ago, the Internet has proven to be the greatest purveyor of news and information in history. From a small band of university researchers sharing documents to more than a billion people around the world connecting in real time, the Internet has proven to be a force multiplier for freedom and a censor's nightmare. Repressive regimes have failed to fully restrict or block access to the Internet. Nevertheless, there are severe challenges to this openness. These challenges are our focus.

It is a top priority for the State Department and for the U.S. Government to do all we can to ensure maximum access to information over the Internet and to ensure minimum success by censors attempting to silence legitimate debate in this global town hall. The U.S. Government and the State Department have been at the forefront of the battle to ensure global access to information through the Internet. We do this bilaterally and multilaterally. My colleague, Jim Keith, will focus on our bilateral relationship with China.

We have actively engaged in outreach with many other countries to find common cause regarding this important matter. Multilaterally, we are engaged in many forums, most recently at the United Nations World Summit on the Information Society, to expand the rights of all people, no matter where they live, to have access to the free flow of information. As the department has focused more energy on this issue, the Secretary has concluded that a task force would be a useful tool to make our strong advocacy even sharper and stronger.

The Global Internet Freedom Task Force announced yesterday will draw upon the State Department's expertise across many bureaus, including international communications policy, human rights, democracy, business advocacy, corporate responsibility, and, as appropriate, relevant countries and regions. The task force will consider the foreign policy aspects of Internet freedom, including the use of technology to restrict access to political content and the impact of such censorship on U.S. companies, the use of technology

to track and repress dissidents, and efforts to modify Internet governance structures in order to restrict the free flow of information.

The task force will also look to ensure that our concerns are being raised at all levels with governments and international organizations alike. We will also work with the private sector and NGOs to help address their concerns in meeting these challenges. The task force will, over the coming weeks and months, make recommendations to the Secretary on policy and diplomatic initiatives to maximize access to the Internet and to help minimize government efforts to block information. We will feed into the robust interagency processes, led by the NSC and the NEC and including our partners at Commerce, Justice, USTR, and other agencies. Our goal in this area may be summarized by our desire to have more people have more access to more information everywhere.

This hearing is obviously an important part of that process. I am pleased with the recent positive statements being made by Internet companies, especially their willingness to work hard on the creation of a global best practices. Of course, they must do much more. Similarly, both in our conversations and in their public statements, NGOs have been very helpful in this effort.

Six decades ago, the Universal Declaration of Human Rights stated:

> "Everyone has the right to information, to freedom of opinion and expression, and this includes the right to freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media, regardless of frontiers."

These rights were reaffirmed most recently at the UN's World Summit on the Information Society just this past November.

We will work with all stakeholders, including, of course, the Congress, to determine the best diplomatic and technical strategies to affirm these rights and practices.

Mr. Chairman, we do not believe that technology alone will lead to the Chinese Government allowing its people to enjoy freedom of expression or the political benefits of the free flow of uncensored information. We will, however, continue to make clear that it is not acceptable for the Chinese Government to continue to suppress speech on the Internet or to foster a climate of intimidation and persecute dissidents. All of the people of China, including the more than 111 million Chinese Internet subscribers, deserve no less. Thank you very much, Mr. Chairman.

[The prepared statement of Mr. Gross follows:]

PREPARED STATEMENT OF THE HONORABLE DAVID A. GROSS, DEPUTY ASSISTANT SECRETARY FOR INTERNATIONAL COMMUNICATIONS AND INFORMATION POLICY, BUREAU OF ECONOMIC AND BUSINESS AFFAIRS, U.S. DEPARTMENT OF STATE

Thank you very much for the opportunity to testify with my colleague from the Bureau of East Asia and Pacific Affairs, James Keith, before these Subcommittees. We have before us a subject of great importance to the Administration and to the people of China. The Internet is one of the great engines of human freedom in the world today, and limits on the spread of information and the use of the Internet to repress legitimate dissent are of great concern to the U.S. Government. Such measures also work against the interests of the Chinese people as they strive to build an "innovation society." We welcome this occasion to discuss with you our views on the Internet in China and U.S. Government efforts to promote the free flow of information via the Internet. The involvement in this hearing of several of

the principal U.S. Internet companies active in China, as well as human rights organizations with an abiding interest in this issue, puts a needed spotlight on a matter of real concern to this Administration, the Congress, and the American people.

In Chairman Hyde's invitation to appear at this hearing, he referred to regulations issued by the Chinese government in September 2005 that are being used to suppress freedom of the press and free speech. The regulations are very broadly written, criminalizing virtually any unlicensed reporting over the Internet of any situation or event that is unflattering to Chinese society or its leadership—at least, in the view of the censors. Among the forbidden activities are "harming the honor or interests of the nation," "spreading rumors, disturbing social order or disrupting social stability" and "inciting illegal assemblies, associations, marches, demonstrations, or gatherings that disturb social order." Clearly, the regulations provide the legal means to censor a very broad spectrum of legitimate speech, and their scope causes great concern.

The new Chinese regulations run counter to the commitments China itself has made to the world community. I had the honor of serving as Co-Head of the U.S. delegation to both phases of the United Nations' World Summit on the Information Society in Geneva in 2003 and in Tunis in 2005. Both meetings concluded with final declarations, which the U.S. worked hard to ensure included strong language reaffirming the critical importance of freedom of speech. For example, the Geneva Declaration of Principles states "that everyone has the right to freedom of opinion and expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." The Tunis Commitment adopted just this past November explicitly reaffirmed the Geneva Declaration and further stated that "freedom of expression and the free flow of information, ideas and knowledge are essential for the Information Society and beneficial to development." Similarly, the Tunis Agenda, unanimously adopted at that same UN Summit, reaffirmed "our commitment to the freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge." China was an active participant in both phases of the WSIS and agreed to all of these WSIS declarations.

In bilateral discussions with Chinese officials, I and many other State Department officials have reminded them of these commitments and expressed U.S. concern over Chinese policies and practices. Senior officials at our Embassy in Beijing regularly do the same, and Mr. Keith will outline these approaches in greater detail. The Administration will continue to remind the Chinese Government of its commitments to giving its citizens access to information, and to make the point that our companies should not be used to persecute political dissenters or to suppress political dissent.

We have also emphasized to the Chinese Government that we do not believe it is in the interests of China for its government to continue to censor the Internet or to establish a climate of fear among Internet users. We continue to urge the Chinese Government to uphold its constitutional guarantee of freedom of expression and to bring its own practices into compliance with international standards. While censorship appears to be incomplete, the vast monitoring effort conducted by Chinese authorities means that users can never be sure whether their legitimate searches for information will be met with intimidation or worse. Such a chilling effect over the world's most dynamic medium of communication cannot help China in its quest to build an innovative, knowledge-based economy. Hampering dissent and interfering with the free flow of ideas does not break the resolve of political dissidents. Instead, it limits China's economic potential at a time when—as the PRC claims—it wants to foster indigenous innovation fueled by increased foreign investment.

The Chinese leadership has sought to draw a line between economic reform and political dissent. That line is an illusion. As Secretary Rice said very recently, "It is very hard to tell people to think at work but not at home."

Following the sentencing of Chinese journalist Shi Tao, the State Department—with much support from our Embassy in Beijing—immediately initiated an intensified dialogue with American companies doing business in China, including those that are appearing before you today. On Secretary Rice's instructions, we expressed to them the Department's concerns about the human rights issues at stake. The message has been unambiguous. With our common interest in establishing the free flow of information in China by using the Internet and other means, we will continue to consult with industry closely.

The Subcommittees will shortly be hearing directly from several of these companies. We applaud recent statements that they recognize the importance of acting responsibly in this very difficult environment and see the value of cooperating with each other to improve the situation of the Chinese people. We have encouraged such

cooperation, and we challenge our companies to leverage their global leadership by developing and implementing a set of meaningful best practices. We want to work with our companies, but the State Department can advocate more effectively for Internet freedoms when U.S. companies conduct themselves in a clear and consistent manner.

Secretary Rice pays close attention to threats to the Internet and its transformational power as a force for freedom. In order to ensure a robust U.S. foreign policy response she established a Global Internet Freedom Task Force (GIFTF) on February 14. The task force will report to the Secretary through Under Secretary for Economic and Agricultural Affairs Josette Shiner and Under Secretary for Democracy and Global Affairs Paula Dobriansky, and will consider foreign policy aspects of Internet freedom, including:

- The use of technology to restrict access to political content and the impact of such censorship efforts on U.S. companies;
- The use of technology to track and repress dissidents; and
- Efforts to modify Internet governance structures in order to restrict the free flow of information.

In addressing challenges to Internet freedom, the task force draws on the Department of State's multidisciplinary expertise in international communications policy, human rights, democratization, business advocacy, corporate social responsibility, and relevant countries and regions. Consistent with existing interagency and advisory institutions and processes, this internal task force will focus the State Department's coordination with the National Security Council, the National Economic Council, other agencies, U.S. Internet companies, non-governmental organizations, academic researchers, and other stakeholders.

We believe that, as President Bush has stated: "Historians will note that in many nations, the advance of markets and free enterprise helped to create a middle class that was confident enough to demand their own rights. They will point to the role of technology in frustrating censorship and central control—and marvel at the power of instant communications to spread the truth, the news, and courage across borders."

Mr. Chairman, we do not believe that technology alone will lead to the Chinese government's allowing its people to enjoy freedom of expression or the political benefits of the free flow of uncensored information. We will continue to make clear that it is not acceptable for the Chinese government to continue to suppress speech on the Internet or to foster a climate of intimidation and persecute dissidents. All the people of China, including the more than 111 million Chinese Internet subscribers, deserve no less.

Thank you again for inviting me here today, and I would be happy to answer any questions you may have.

Mr. SMITH OF NEW JERSEY. Thank you very much, Ambassador Gross.

Mr. Keith.

TESTIMONY OF MR. JAMES R. KEITH, SENIOR ADVISOR FOR CHINA AND MONGOLIA, BUREAU OF EAST ASIAN AND PACIFIC AFFAIRS, U.S. DEPARTMENT OF STATE

Mr. KEITH. Thank you, Mr. Chairman. I would like to add my thanks for including us in today's hearing and want to commend the Subcommittee for shining the light on these practices. If I may, I would also like to point toward the work that the CECC has done under Chairman Leach's co-sponsorship. We have used much of their information already and will continue to do so in showing the Chinese Government that there is a partnership between our two branches of government in seeking to advance our goals in China.

Again, the way we have put that, in one respect, is that it is a top priority for us to maximize access to information over the Internet and minimize success by censors to control it. Another way of putting that, if I may paraphrase something that one of the Members said a moment ago, is we certainly need to find a way to sus-

tain the promise of the technology without acquiescing to the intent of the censors.

This is a top priority for us. We have direct instructions from the Secretary of State to advance this agenda, and, in a broader perspective, we are led by the President in our engagement with the Chinese on human rights objectives. He has been the most forceful spokesman for advancing our human rights agenda in China, including during his recent trip to the region just at the end of last year.

I would say to you also that our assistant secretary for democracy, human rights, and labor, Barry Lowenkron, is in China today. He has already made points reiterating our strong commitment to precisely this question of maximizing access to information over the Internet and limiting the censorship which is increasing in China, and he has raised specific cases, as have the Secretary, the President, Ambassador Rant in Beijing, and other senior Administration officials and will continue to do that, I can assure you.

In addition to that, we are looking for ways to address systemic reform in our human rights agenda. We will not lose sight of any of the individual cases, of course, but we also have to work toward the long-term, looking for ways to bring, both bilaterally and multilaterally, pressure to bear for China to address the systemic problems that exist today. These are problems that, as you know, Mr. Chairman, we have addressed in our human rights reports and will continue to do so every year, including this one.

Just to take one example of the kinds of things that we are raising as both individual and systemic issues, jamming of VOA and RFA are activities that we have protested, will continue to protest, and have tried to make the case to the Chinese as to why this is not in their interest in the long term.

We will continue to bring public attention to all of these negative or backward-looking activities on the part of the Chinese Government while at the same time trying to point toward more productive and promising avenues in the future.

I commend also the Subcommittee's attention to the distinction between negative and backward-looking activities on the part of the Chinese Government and the success and prosperity of the Chinese people that we hope for. We look to sustain that distinction because we want the Chinese people to know that we are looking for a China that succeeds, and we are looking for ways to help them make the right kinds of accomplishments and achievements not only on their own but through the efforts of the Chinese Government over time.

It has been the President's contention that our pressure on the human rights agenda with the Chinese is precisely designed to help them succeed. In fact, economic modernization in China depends upon, over time, the Chinese Government opening itself up not only in the economic area but also in the political area. This has been an important motivation for us in engaging the Chinese Government on our human rights agenda.

Like many voices in China, some of whom I know will be represented in later panels, we anticipate the Chinese Government will find it very difficult, in fact, perhaps an exercise in futility, to try to control the flow of information into China. China itself as-

pires to succeed as a knowledge-based economy, and as has been pointed out earlier, just this week, former senior government officials and scholars have, in China, pointed to the problems with censorship and China's own interest in advancing political reform and advancing government decisions that would limit intervention into areas such as the Internet.

In fact, one commentator this week, as quoted in the *New York Times*, described China's current situation as a censor's nightmare, given the hundreds of millions of consumers who make up the market for information in modern China.

So our message is that we want to work with the Congress. We look forward to opportunities to persuade the Chinese Government that this is the direction it ought to move in, and I can assure you, this will continue to be a high priority for us, both in terms of our multilateral engagement as well as our bilateral engagement with the Chinese.

In sum, our perspective is that Chinese censorship is increasing. It is wrong, it is contrary to China's own interest, and, in our view, ultimately it is futile. Thank you, Mr. Chairman.

[The prepared statement of Mr. Keith follows:]

PREPARED STATEMENT OF MR. JAMES R. KEITH, SENIOR ADVISOR FOR CHINA AND MONGOLIA, BUREAU OF EAST ASIAN AND PACIFIC AFFAIRS, U.S. DEPARTMENT OF STATE

Mr. Chairman, Committee members, thank you for inviting me to participate in today's hearing on the Internet in China. I believe this hearing has had the salutary effect of helping us focus our approaches to the many issues involved in this complex subject. As the Secretary made clear in her February 14 announcement of a new government task force to lead the way in resisting challenges to Internet freedom, the right to freedom of expression is firmly anchored in international law and in multilateral conventions and is an American foreign policy priority. We intend to sustain a robust foreign policy response to these challenges. I welcome the opportunity to join with you and my colleague, Ambassador David Gross, the Deputy Assistant Secretary of State for International Communications and Information Policy, to help the subcommittee explore this important topic.

China's policy of economic reform and opening up has resulted in the integration of China into the world community in ways more profound than many would have predicted, though the degree and scope of integration has varied by sector and subject. Nowhere is this better seen than in the Chinese government's efforts to adapt to—and control—new technologies. What the fax was in the late 1980s and the cell phone has been a decade later, so the Internet has become in the 21st century—a vital force for spreading information and exchanging ideas. China's leadership recognizes the centrality of the Internet and the free flow of information in providing the economic data to make China's market-oriented reform possible, but its effort to regulate the political and religious content of the Internet is counter to our interest, to international standards, and, we argue, to China's own long-term modernization goals.

We believe China will not achieve its ambitious development goals unless it opens its political system further and allows the full participation of its citizens in the political process. There are abundant tools available to the Chinese people in the technological and information sector to create the stable, prosperous and just society that would serve China best. In 1997 the number of Internet users in China was approximately 600,000. Today there are 111 million internet users in China—still just 8 percent of China's population—making China second only to the United States in total number of users. As Beijing looks at the world around it, it sees a flow of information into China—not just from the Internet but also from cell phones (China has more than 350 million of them), text messages and a large and growing foreign business, student and tourist presence—that challenges the government and society to conceive and formulate new ways of doing business, interacting socially, and relating to one another.

We are firm in the conviction that the flow of information into and throughout China will not reverse itself. As the President said in Kyoto, Japan in November,

as China reforms its economy, its leaders will find that once the door to freedom is opened a crack, it can not be closed. The President, Secretary Rice, and senior Administration officials remain deeply engaged in our efforts to challenge the Chinese to open the door further and think creatively about a future in which the ideas of individual citizens help to keep China at the cutting edge of 21st century development.

Regrettably, China's leadership efforts to monitor the content of the Internet have accelerated in the past year, sending a chilling message to all Internet users. Beginning in March 2005, PRC authorities began to enforce the "Computer Information Network and International Internet Security Protection and Administration Regulations" which require that all website operators register their sites with the local Public Security Bureau within 30 days of beginning operations. The Chinese government has shut down thousands of sites for failing to register. Then in July, the government issued new regulations requiring instant message users and bloggers to use their real names.

An attempt to exert even greater control came in September with "The Rules on the Administration of Internet News Information Services," promulgated by the State Council Information Office and the Ministry of Information Industry. These rules—like those dating back to 1999 when the Chinese government first sought to control what Internet Content Providers could and could not publish—try to ensure that ideas that do not have the government's imprimatur or that challenge its authority do not take root in China. The rules are hard to interpret, especially when they mandate that Internet News Information Service Work Units or organizations may not include content that jeopardizes the security of the nation, divulges state secrets, subverts the national regime, jeopardizes the integrity of the nation's unity, harms the honor of the nation, or disturbs social stability, among other cautions. These vague and variably interpreted restrictions limit search results on ICPs operating inside China about, for example, the Tiananmen Massacre, the Dalai Lama, democracy, or human rights, to name just a few terms that are subject to content control.

Even issues that appear to be somewhat distant from the subject of political reform can be captured by the government's overriding focus on social order. For example, it is clear in retrospect that the government initially sought to restrict public awareness of public health and environmental issues such as the SARS outbreak in 2003 and the recent Songhua River spill in northern China.

We have raised our concerns about content control and about the treatment of Internet activists repeatedly and firmly with the Chinese government.

- We have expressed concern about the cases of journalists, editors, and writers detained or imprisoned for expressing their view or sharing information on the Internet including Shi Tao, who was sentenced to ten years for forwarding Chinese government instructions on how the media should cover 16th Anniversary of the Tiananmen Massacre.
- We have told the Chinese government that we are also deeply troubled that another individual, Li Zhi, was reportedly imprisoned earlier for expression of his views over the Internet.
- In addition, we have protested the sentencing of Yang Zili, an activist who was part of an Internet group discussing political reform, and Li Changqing and Yang Tianshui, who were both arrested for their Internet-based writings.
- Censorship and restrictions on media outlets, including the Internet, have been the subject of numerous and frank protests to the Chinese—including one by our Charge in Beijing on February 9—and will be a key topic of discussion when Assistant Secretary for Democracy, Human Rights and Labor Barry Lowenkron holds meetings in Beijing, which began today. He will express our deep concern about China's efforts to control the free flow of information in violation of international commitments, including those made at the World Summit on the Information Society to "seek, receive, impart and use information, in particular for the creation, accumulation and dissemination of knowledge." Ambassador Gross has addressed that matter here today.

Despite the presence of thousands of government monitors—perhaps as many as 25–30,000 by one estimate—and the involvement of more than 20 ministries and government organs in "managing the Internet," China's success in its attempts to control this technology has been limited at best.

- While Internet use and content is officially restricted, registration requirements and enforcement vary by Internet café and by city in China. Of course, computer savvy Internet users can usually get around the censors by using any number of proxy servers. In fact, one commonly used service,

Anonymizer, a leading online identity protection technology, has just announced that it is developing "a new anti-censorship solution that will enable Chinese citizens to access the entire Internet safely and filter-free, and also free from oppression and fear of persecution or retribution. The new program is expected to be available before the end of the first quarter 2006.

- Some sophisticated Chinese Internet users are adept at using code words or symbols to get their views across without triggering key word filters.
- American officers in China have found that news containing politically-sensitive words can be accessed, though its availability varies day-to-day and site-to-site.
- Many well-known English language websites including the *New York Times* and *Washington Post* are accessible but others including Voice of America, the BBC, and Reporters Sans Frontiers are consistently blocked. We have and will continue to protest these blocks.
- The Department of State's Embassy and Consulate sites, though subject to intermittent blocking, are generally available and provide access to U.S. policy statements and the Department's Human Rights Reports.

Of course, censorship efforts need not be widespread or effective across the board to achieve their aim. Censors just need to arrest and sentence a few prominent individuals to send a chilling message. But I believe, as do many in China, that controlling the Internet to the extent that the Chinese government has sought to do is likely to be futile in the long term. As Professor Xiao Qiang, the leader of the Internet project at the University of California at Berkeley and from whom you will hear later in this hearing, is quoted in the February 9 *New York Times*, "Symbolically, the government may have scored a victory with Google, but Web users are becoming a lot more savvy and sophisticated, and the censor's life is not getting easier." The *Times* goes on to note that "Microsoft alone carries an estimated 3.3 million blogs in China. Add to that the estimated 10 million blogs on other Internet services, and it becomes clear what a censor's nightmare China has become."

I expect that market forces will continue to push China toward a less restrictive approach to the flow of information. The international and domestic business communities in China will continue to demand not only the hardware for the information age, but also the software, including unfettered access to the Internet and seamless broadband connections unburdened by filtering and other government efforts that render commercial operations less effective, reliable, and efficient.

Mr. Chairman, we will do our best to shape public and private interaction with China in ways that advance fundamental human rights, including those for Internet users. This is a central tenet of the Secretary's new task force on Internet Freedom. I assure you that this Administration will engage the Chinese government on these issues in ways that promote American values and ideals.

Mr. SMITH OF NEW JERSEY. Thank you very much, Mr. Keith.

I would just advise the Members we will be operating under the 5-minute rule for panel 1.

Let me just ask, and that goes for the Chairman as well, earlier, Mr. Meeks and others have said that somehow the Chinese and the companies operating there are just abiding by the laws of China. As you pointed out, Ambassador Gross, the most recent regulations provide the legal means to censor a very broad spectrum of legitimate speech, and things like spearheading rumors, disturbing the social order, absolutely catch-all phrases, and I am wondering if you can tell us—we have seen corporations in the past live and, unfortunately, thrive in dictatorships. South Africa comes to mind. Those companies that have done business in Sudan and other places where gross violations of human rights are commonplace.

We know for a fact, and Manfred Nowak, the Special Rapporteur on Torture, just gave us a fresh iteration of that after his visit and report in early December, and he is a very eminent human rights person, and he said torture is widespread in China. If you go to the Laogai, you can count on being tortured. He also said that many of the people with whom he met were very much intimidated, would not talk to him, including others—this idea that somebody

on the street gives a glowing rendition of how things are in China is basically the Potemkin Village, especially if you cross the line and speak out on fundamental human rights and desire freedom or religious freedom, at that, in the countries.

So my question is, the new Global Internet Freedom Task Force that you have announced, and I applaud the Administration for doing this; how will it deal with this whole issue of U.S. corporations partnering with the secret police? We know of Shi Tao. We know of others, but as I said in my opening comments, that is probably just the tip of the iceberg. There are so many who are probably languishing and being tortured in the Laogai, and I, frankly, was in a Laogai. Frank Wolf and I visited Beijing Prison No. 1 in the early 1990s after Tiananmen Square and saw about 40 Tiananmen Square activists who were there with shaved heads. It was reminiscent of the concentration camps of a half century ago.

I would also say to all of my colleagues, if you have not read IBM and the Holocaust—Clarence Page, the syndicated columnist, suggested just a day and a half ago that I read it—I have gotten through about half of it, and it is an indictment of that collaboration, an almost see-no-evil view that some take that somehow they are on the side of efficiency and making the trains run on time and maybe even liberalizing a society when, in fact, they are actually aiding and abetting a dictatorship to be more potent, have a higher degree of efficacy in promoting its repression. It seems to me these are like tools in the hands of a repressive regime. Now they can do that much better in terms of a dragnet, if you will, with regard to its people.

So if you could speak to that issue. What would this new initiative do with regard to partnering with the police to crack down on dissidents?

Mr. GROSS. Sure. Let me respond with a couple of thoughts. The new task force will allow us within the State Department to sharpen our focus on how to deal with these classes of issues. We have a lot of resources and a number of tools that we have.

One of the tools that we are going to be looking very closely at trying to be more effective in using is reaching out to other governments. As has been noted by many of the Members this morning, although the focus today is on China, we should not forget that this is a problem that is broader than China. And, similarly, although we have U.S. companies in focus today, this is also a problem that is broader than just U.S. companies. There are many other companies around the world that are involved in the same sorts of activities, and it is a global, competitive marketplace.

So what we have already begun to do, but we are looking to do more of, is to reach out to our companies to better understand what is going on to make sure that we understand what the facts are, to promote, as we have today, and we will continue to do, global best practices that have been the source of discussion this morning, to reach out and to talk to NGOs, both domestic and abroad, to better understand their views and their desires. I was particularly impressed by a number of the comments that were made before the caucus earlier this month, some of the very thoughtful ideas, including the opportunity to work together, both companies and NGOs, together with government on these projects.

So we look to outreach and to use the task force to reach out to other governments around the world that have similar values to those that we have, to try to work collectively, and, most importantly, to try to find the efficient ways to deal with this problem. We recognize very much that words alone are not what this is about. What we really want to do is have actions and results, and we are going to be looking for those good ideas from any quarter, domestic or foreign, and to listen carefully and then to implement strongly.

Mr. SMITH OF NEW JERSEY. Let me just ask you, if I could, the censoring of U.S. sites. As I think you heard in my opening comments, and I think we have shared some of the broad outlines of the legislation, the Global Online Freedom Act of 2006, one would be to put e-mail service outside of a repressive country so that the ability of the secret police to have access to is at least mitigated and hopefully prevented.

We also would provide for no censoring of U.S. Government sites. Obviously, Radio Free Asia and Voice of America provide a very valuable insight for those who do not get uncensored information. We would also provide that U.S. Internet service providers could not block those sites, and I am wondering how you might feel about that because it seems to me, I went and looked at several of google.cn's sites and was almost shocked, certainly was dismayed, to see that you not only were blocked on some occasions when you did "China human rights" or something of that kind; you went to the disinformation site, People's Daily, china.com.

For instance, I asked about Manfred Nowak, a very esoteric type of search question, and rather than getting his report on the Google Chinese search engine, I was sent right to People's Daily where he was criticizing the United States for Guantanamo. Certainly, his criticism should be looked at and deciphered, but you did not hear anything about what China was doing.

So on the U.S. sites, your thoughts on that and basically on what you may know already about our bill. Do you think it is valid and needed?

Mr. GROSS. Let me start off, and then let me turn it over to Mr. Keith.

Of course, the Administration would be happy to provide lots of feedback on the bill, and I have not had a chance to look at it, although I, of course, have heard your comments about that. I think, obviously, there are a lot of very important and very good ideas there.

If I may, and at the risk of sounding somewhat nontechnical, even though my expertise is technology, one of the things as I have visited China that I hope that you all will keep an eye on, as we are keeping an eye on, is that the methods used by the Chinese Government are not just technologically based. For me, at least, one of the most sobering and chilling aspects was the use of people to police this; that is, not only the approximately 30,000 cyber police that people have talked about, although no one really seems to know the exact number, of course, but also the use of active registration, people looking at what it is, people are typing it as they type it in, and, in particular, the idea that you may never know

whether or not your e-mail or your Web searches are, in fact, being looked at at any given time.

So it is not just a question of technology. In some respects, oddly and perhaps somewhat counterintuitively, I almost wish it were because then the technological solutions we would all hope for may be there. But I hope we all keep in mind the even, to my mind, more difficult set of problems is how do we deal with that mindset? How do we deal to try to convince the Chinese Government that at their core they are going the wrong way, and even their nontechnical, but sometimes very effective, approaches are, in fact, just as difficult and just as counterproductive.

Mr. KEITH. Mr. Chairman, I would add that ultimately the question you raised relates to the rule of law and transparency in China. This, of course, is a key area of our interest and an area where both the public and private sector in the United States are deeply engaged in China and trying to advance, with some success in some areas and some real obstacles in others, the deepening of the roots of the rule of law in China.

I think, looking at the specific question you raised, while one cannot count on this, and all we have is anecdotal evidence, it is certainly true that the ingenuity of the consumers in China is shining through, and that is that it is possible to get a wide range of information, including from major publications and through official U.S. Government sites without pointing to directly to specifics because the last thing we want to do in this setting is provide a roadmap as to what ought to be blocked or what is not being successfully blocked. Of course, our position is that nothing should be blocked, and we will keep working in that direction.

I see it as part of our goal is to try to create the atmosphere in which our companies can work, and that atmosphere should be one based on the rule of law and should be one in which any changes that the Chinese Government announces are transparent to all consumers, both Chinese and outside.

So that is our goal, sir. I have to admit, as robust as our engagement on these subjects has been, we have to be judged by results, and we are as frustrated as the Congress is in many areas by the results.

Mr. SMITH OF NEW JERSEY. I have an additional six questions, but in the interest of time, we will submit them to you and ask if you could, as quickly as possible, get back to us.

Mr. KEITH. Yes, sir.

Mr. SMITH OF NEW JERSEY. Mr. Payne?

Mr. PAYNE. Thank you very much. I would be curious to know, in your opinion, how do PRC's citizens view the impact of the Internet on China's society and politics? Do you think they perceive the Internet as a potential political tool?

Mr. KEITH. Sir, if I may, I think the answer to the question, as was indicated by the Chairman's comments, has to be divided into different categories; that is, in many respects, the Internet is a tremendous tool for the average Chinese user, particularly as has been commented upon in many areas where the government is not interested in effecting control.

I think it is quite clear that both international and domestic firms in China see the Internet not as a luxury but as an absolute

necessity in the 21st century doing business, and, as such, the Chinese Government has to be aware that the infrastructure for attracting investment, for attracting people to do business in China, depends in part on the free flow of information, including through the Internet, that companies now expect to be able to do this kind of work in order to conduct their business, and they can do it in Tokyo, Seoul, Shanghai, Singapore, many different places. So the work of the marketplace is helping to extend pressure on the Chinese Government.

I think it is absolutely the case that whether you look at cell phones or text messaging or even going back to faxes to just give a sense of how quickly the technology is changing here and how rapidly the landscape can change underneath you, all of these technologies have been an integral part of spreading of information in political or even only indirectly political areas.

To give two quick examples, in terms of protection of the environment, the recent oil spill in China was made public through use of the Internet, and had it not been for that, might have been more difficult for the public to be aware of it.

Then to go back into history a little bit further, the initial news about the SARS epidemic, at that time, a completely unknown and new disease, came through use of the Internet.

So it is absolutely a critical part, both in terms of the aboveground, legitimate, from the Chinese perspective, way of doing business as well as the informal network of communication not only between China and the outside world but also, very importantly, throughout China.

Mr. PAYNE. Do you think that the SARS epidemic; was the government still trying to suppress that information, or did it come out just because of Internet use and the curiosity, et cetera?

Mr. KEITH. Sir, the news came out, and the government responded to it. I would say that the government responded with alacrity to it, in fact, over time. We have seen, looking back, that the government was quite decisive once the information was out in public, but it would not have come out as quickly as it did had it not been for the technology that was used to spread the information.

Mr. PAYNE. There has also been sort of silence on HIV/AIDS in the past in the PRC. To your knowledge, has the Internet pushed the government to acknowledge it has a problem and start to deal with it?

Mr. KEITH. I think it has been part of that solution. Sir, I would say that the history on HIV/AIDS with the Chinese Government is one in which it has become increasingly transparent such that that is now more of an example of the kind of thing it should be doing as opposed to what it should not be doing. In the very beginning, the Chinese Government was very reluctant to admit to statistics and that sort of thing.

What really drove HIV/AIDS, I think, was the Chinese Government's recognition that the transfer of narcotics, and international crime being involved in that, from the Golden Triangle through southern China was inimical to their own interest, and, therefore, they started to engage very directly with us and with many other

countries and with NGOs, including the Gates Foundation, to try to advance their own interest in trying to control it.

So I would say, in that case, with HIV/AIDS, the Internet was not the major driver; it was China's recognition that it was quite vulnerable.

Mr. PAYNE. I, several years ago, had the opportunity to fly up through Burma and went up to the area that borders China and the sort of vice that goes on, the casinos in the middle of nowhere, prostitution and so forth, and I would hope that the government would look in terms of trying to crack down on the Chinese citizens that go across the border for these activities.

Let me just ask this final question, since time is of the essence. To your knowledge, is there a debate within the PRC Government on how to handle Internet censorship? Are there political or social or economic interest groups in China who would be more likely to support fair mass media in general and Internet in particular? Which groups would likely oppose it, and how far do you think they will go, push the envelope, without feeling repression from the government? Are there any groups that are pushing for this?

Mr. KEITH. Sir, I will try to answer as succinctly as I can. This, of course, is one insight into a much larger question in China in terms of its economic modernization and opening up and the different pressures that exist from different parts of the bureaucracy for a wide variety of reasons, some relating to public order and social order from their perspective and some relating purely to business practices and the desire of some elements in the bureaucracy to protect their opportunity to operate in a commercial environment.

So it is certainly the case that, speaking in very general terms, that there is an overall commitment to economic reform and opening up in China, but there is a debate among all of those without opening up the question of whether China should back up in terms of its modernization.

There is a debate as to how fast and how far it should go. The scope and pace of reform, I think, is certainly debated within China among the economic ministries and among those ministries responsible for public security. I think that debate is joined, and it is certainly the case that we want to appeal to those who are making the case for economic reform and modernization depending on the free flow of information.

Mr. PAYNE. Thank you, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. Chairman Leach?

Mr. LEACH. The Internet issue raises rather extraordinary trade issues that we have never had before and whether we should as a part of our trade policy have protection of a free Internet. Has the Administration given that any thought?

Mr. GROSS. The answer is yes. We have had conversations, both within the Administration and with companies and with academics, about this subject. I would leave it to our colleagues at USTR to make the judgment about this thing, but it has been an area in which there has been discussion and discussion about it.

Mr. LEACH. I would just like to raise one philosophical notion because the Chinese pay attention to hearings of this nature. As we know, the executive has attempted to identify the word "democ-

racy" as part of its foreign policy agenda, and, frankly, that is American heritage; it is nothing unique to this Administration; it is our heritage. But the word "stability" is very important to the Chinese, and the question is what is destabilizing, and what is stabilizing? In a general framework, I think it would have to be said that the United States' advocacy of openness of information is not intended to be destabilizing, that as a general framework, the spread of knowledge is a stabilizing phenomenon, not a destabilizing one.

I only raise this because there is often a question of motivations, and I hesitate to get this particular discussion characterized as one aimed against a regime. It is aimed against certain policies of countries—a principal one is China, but it is on the side of the Chinese people, which becomes a stabilizing rather than destabilizing factor in that society as well as within our relations with it. Now, is that a perspective that you would share, or would you take another tack at this?

Mr. KEITH. Mr. Chairman, that is an articulate description of precisely what the President has told the Chinese Government, I think, repeatedly, that, in fact, our perspective is that our engagement on human rights in China is aimed at the success of the Chinese people, that we want to see a stable and prosperous and successful Chinese people, and our strong conviction is the way to get there is not only through economic reform and opening up but also these kinds of issues that have been labeled as political reform, but they, in some cases, are administrative reform and in some cases relate to areas that are not as sensitive to the Chinese Government but also are directly involved in people's equal access to justice and due process.

We are working across the board in these areas, those that the Chinese deem most politically sensitive and others, with precisely this intent in mind; that is that for the Chinese to fail to allow for the views and feelings of their population to be registered in a meaningful way with the government leads to more instability, more of the kinds of incidents of problems in the countryside that have been reported on and are, in fact, a priority for the government in the upcoming National People's Congress this March, when, as the Chairman may know, the Chinese Government will focus on these imbalances that exist in Chinese society today.

Mr. LEACH. I appreciate that, but I am trying to take this a little bit outside the discussion of human rights, although an individual right is freedom of the press. But what we really have here is something more extraordinary. This is the right to knowledge, which is of a distinctive nature, and I just want it very clear that in our discussions of Internet issues we are talking about the precision of right to knowledge and how knowledge can be used, and it both is stabilizing and handicaps a society if they do not allow citizens access to knowledge. Does that seem to be a perspective that is the driving force behind this new task force, or is it something very different?

Mr. GROSS. I would say it is an important part of that. I have had some personal experience on exactly the issue that you are raising. When we were negotiating for both phases of the UN World Summit on the Information Society, we had very candid dis-

cussions with our Chinese colleagues and colleagues around the world, so we recognize the apparent tension that there may be between the issues of stability and free flow of information.

I think, without speaking for them, of course, I think ultimately we were able to get the very, very strong language that we did because there is a recognition, particularly in a world in which most economies, certainly the Chinese economy is trying to become an economy based on innovation, that access to information broadly construed is key for future stability of economies and of societies, and I think that is one of the themes which we seek to work with the Chinese Government and with many other governments around the world.

We believe that this is not something to be frightened of or to be fearful. It does not lead to instability but rather, in fact, leads to a much more stable environment for everyone.

Mr. LEACH. Thank you very much.

Mr. SMITH OF NEW JERSEY. Thank you, Chairman.

Mr. Faleomavaega?

Mr. FALEOMAVAEGA. Thank you, Mr. Chairman. Before I raise a couple of questions here with the members of our witnesses, I want to offer my personal welcome and compliments to Mr. Keith, whom I have had the privilege of knowing a couple of times on my visits to Shanghai and did a fantastic job in representing our Government there as consul general. I am very happy to see you here back in Washington.

Mr. KEITH. Thank you very much.

Mr. FALEOMAVAEGA. It is somewhat ironic, Mr. Chairman, that we here on this side of the aisle seem to be complimenting more the presence of our corporate community there in a place like the People's Republic of China promoting, at least in some form, a sense of advocacy, of public diplomacy, if you will, and the presence there of our companies seems to put a brighter light on other aspects of our policies throughout the world, at least in a country like China despite all of the problems that we are faced with, like any other country.

I wanted to ask both Mr. Keith and Mr. Gross, suppose we do pass a law to mandate that our high-tech companies leave China because of these repressive reports that we get in terms of censorship and our companies having been forced to reveal the identity of those, especially the Chinese, who are employed by these companies because of violations of some information given here. Let me ask you this. How many other companies do business in China besides those who come from the United States? Do we have competition from the corporate communities in Europe or others? Are we the only high-tech companies that do business in China?

Mr. KEITH. Sir, we are not the only companies, and, in fact, Chinese companies are among the competition.

Mr. FALEOMAVAEGA. What is the total investment of our high-tech companies that do business in China right now as of now?

Mr. KEITH. I guess I would have to know a little bit more about precisely how you wanted to break that down, but I can take that question for you, sir, and get you an answer.

[The information referred to follows:]

WRITTEN RESPONSE RECEIVED FROM MR. KEITH TO QUESTION ASKED DURING THE HEARING BY MR. FALEOMAVAEGA

According to statistics from the U.S. Bureau of Economic Analysis, at the end of 2004 total U.S. direct investment in China was $15.43 billion. Of that, $3.85 billion, or about 25% the total was invested in the chemicals, computers and electronics products, electrical equipment, appliances, and components, and information sectors. I note that BEA statistics show a significantly lower amount of U.S. FDI than Chinese numbers as the BEA does not include U.S. investment that flows through Hong Kong.

Mr. FALEOMAVAEGA. What is the total investment of our total corporate presence there in China? How do we rank, second, third among the countries of the world that do business in China? I am curious.

Mr. KEITH. Our cumulative investment is among the top in the world. We are behind those overseas Chinese in Hong Kong and Tapei who, to some degree, include round-tripping investment, that is, money that comes out of China goes to Hong Kong or Tapei and then back into China, but we certainly are among the top investors in the world in China.

Mr. FALEOMAVAEGA. Can we kind of wing it? Can you give us some rounded out figures in terms of how much is our total investment there in China? See, I am a free enterprise supporter in that regard, if you will.

Mr. KEITH. Sir, on the order of $30 billion.

Mr. FALEOMAVAEGA. Thirty billion dollars.

Mr. KEITH. If I have to stand corrected on that, sir, I will certainly get that to you.

Mr. FALEOMAVAEGA. How does that compare with other high-tech companies from other countries? I suppose Europe is probably our biggest competition as far as high-tech is concerned.

Mr. KEITH. Yes, sir. Well, cumulative investment of $30 billion, I think, across the board. The EU is a competitor. For example, just to take one case in point, Boeing and Airbus are very strong competitors, and that includes a great deal of technology component in the product. We are increasingly, especially in the energy sector, competing in the region. The Australians and the Indonesians are heavily involved in China.

Of course, in the manufacturing area, it tends not to be as high-tech, and that is where many of the competitors are for us coming out of southeast Asia and raw material being shipped up to China and then assembled in China and sent off to the international marketplace, including a large portion of it to the United States.

Mr. FALEOMAVAEGA. One of the ironies that we find ourselves in, there is always this constant bickering and public defiance between Taiwan and the People's Republic of China. What the world does not seem to know is that between Taiwan and China they have an unofficial, $100 billion trade going on. It is one of those contradictions that I find difficult myself to know.

Let me ask you one more question, and I know my time is almost up. The Olympics are coming up in the year 2008. Do you suppose that the presence of these high-tech companies might have some semblance in terms of really letting the world—do you think that the Chinese Government would really allow our high-tech companies to be part of this dissemination process of telling the world how great China is? Would the government have a tendency to put

more suppressive policies, and the fact that Google and Microsoft and Cisco Systems, these companies that are part of the this technological, high-tech information technology that we have in the world, do you suppose that the Chinese Government might have someone because this is what they wanted to do—do you think that there may be some change in understanding that this could really be a plus for them rather than put it in the more negative concerns of my good Chairman here that you want to arrest people and put them in prison for 8 years just because they have violated some semblance of the security risk or whatever it is that they are concerned about?

Mr. KEITH. Sir, if I may answer in two parts, it is absolutely clear that the Chinese Government wants the Olympics to have a symbolic effect along the lines that you describe and that they are clearly motivated to move in that direction.

I think part two has to be the long-term perspective that it is going to take, in my personal estimation, generations for us to see the change in mind-set that is associated with deeply rooted perceptions of the rule of law and operation of the rule of law.

So I think we have to keep the short- and long-term objectives in mind at the same time. Clearly, the Olympics is going to be, in the Chinese mind, a watershed, and there is every reason to believe that they are motivated to try to create that impression in the international community.

Mr. FALEOMAVAEGA. As a follow-up to my good Chairman and colleague, Chairman Leach, had said earlier about not so much linking to the government, but basic philosophical and ideological problems that we sometimes get with the cultural nuances. I remember a couple of times when we visited Beijing, and we were complaining to the Chinese leaders about human rights, and as we got to really understanding, well, what do you mean by human rights? They have a totally definition of what human rights is. To them, human rights is making sure that there is food and shelter for the people, and, to them, that is the primary concern in the minds of the leaders. How do you go about feeding 1.3 or 1.4 billion people?

I would like to offer this challenge to our own country and our own Government leaders. We are having a problem feeding 300 million living here in this great nation of ours. We cannot even provide health insurance for some 46 million Americans.

I wanted to kind of lend that sense of my trying to understand the nuances and how we deal with a country as complex, a country who really we have to deal with when dealing with North Korea, with Iran, with Russia, with India. We cannot just point the other way and think that this country is going to go away because it is not.

I did not mean to direct my questions just to Mr. Keith. Mr. Gross, this great plan that Secretary Rice has decided to put in as an integral art of our State Department, what are some of the pluses that you see? Do you have any timelines that say, hey, in 5 months' time, this is what we are going to do, and is it just toward China? I am sure there are other countries that have similar policies. What about countries in the Middle East? Do they have security problems and censorship as well? They are not very demo-

cratic, with the exception of the State of Israel. Are there other countries that have the same problems that we are dealing with as China?

Mr. GROSS. Absolutely. If the question is whether or not there are other countries that do not subscribe to the free flow of information and the importance of that, the answer, unfortunately, is absolutely yes. They are not regionally specific. There are, unfortunately, a good number of those countries, and it is for that reason why the Secretary's establishment of this new task force is so important. It is not focused on any one country, and it will look within the department to use the resources of our regional bureaus to identify those countries and then to work on them.

We think that that work needs to be specific and unique to each country because each country has its own set of challenges and own set of opportunities, and we look forward to finding those solutions and working creatively not only within the department but then reaching out and working collegially, as I have said before, with other governments and others on this very, very important set of issues.

To simply answer your question, yes. Unfortunately, this is a broader problem than just one country.

Mr. FALEOMAVAEGA. And if we were to pass a law putting the hammer on China, then we would have the cooperation of the State Department to tell us that there are other countries that we are having similar problems as we are with China at this point in time.

Mr. GROSS. I think the Congress can always feel assured that the State Department is here to help.

Mr. FALEOMAVAEGA. Thank you. Thank you, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. Thank you.

Ms. McCollum?

Ms. MCCOLLUM. Thank you, Mr. Chair.

I am assuming Taiwan's Internet access use is similar to what we would experience here in the United States or in the European Union or Australia. Would I be correct in that assumption?

Mr. GROSS. If the question is in terms of the free flow of information as compared to the percentage of penetration, the answer would be yes. In fact, actually, there are a lot of very interesting things going on in Taiwan about the use of technology, and there is a lot of dynamic use of and high-penetration rates.

Ms. MCCOLLUM. And Hong Kong? What can you tell me about Hong Kong?

Mr. GROSS. Let me start, but I, of course, am sitting next to an expert on Hong Kong.

Ms. MCCOLLUM. Either one of you.

Mr. GROSS. Hong Kong is an extraordinarily dynamic place in terms of the use of technology and has been for some period of time.

Mr. KEITH. It is certainly one of the most wired cities in the world and very deep penetration into the account.

Ms. MCCOLLUM. Has there been any movement by the Chinese Government to influence what is going on with Internet use in Hong Kong?

Mr. KEITH. Not that I am aware of.

Ms. MCCOLLUM. I am going to show my lack of Internet savvy here real quick probably, so do not be afraid to say that you are mixing things up here. If I am a United States business, Minnesota Mining & Manufacturing, for example, and I am in my offices in mainland China, and as an American citizen, as an employee of that company, is my Internet access restricted by the Chinese Government?

Mr. KEITH. I am sorry. If I could just clarify. You are an American citizen working in a company in China. You have access to the same systems in Chinese that everyone else does, is my understanding; that is, you go through the same portals to the international community that the Chinese Government has structured, so you are captive by that.

Ms. MCCOLLUM. So, in other words, I am filtered. My access is restricted.

Mr. GROSS. I think probably the perhaps somewhat unhelpful answer is that it depends. It can be as restrictive, but sometimes it is not.

One of the things which we have found, and this is true in many situations in China, is that it varies from time to time and place to place. Part of it depends upon the way in which the company has its network engineered. There are ways in which it can avoid some of the same problems you would see, for example, in cyber cafes in other parts of China. Having said that, so far as I am aware, almost all of it eventually has to come through a certain gateway, so certain filtering occurs at those gateways. There are some exceptions to that rule, but I think, by and large, the answer would be yes.

Ms. MCCOLLUM. And there is going to be another panel up probably, so whether I am a university teacher maybe working on a paper while I am over there or a U.S. citizen working out of something like that, I may or may not find myself restricted.

I have a policy question. I do not want to revisit the controversy discussion that we were having up here among us, but at the same time, I think what we do, what we say, how our words are interpreted as government-to-government relations, there is a *New York Times* article from February 14 in which a Chinese official is cited on here, and part of his job is he is the information office of China's state consul and cabinet.

Mr Liu says, "The Chinese effort to regulate content on the Web is aimed primarily at preventing the spread of pornography, content harmful to teenagers," and he says, you know, we have the same concerns. We are trying to do the same things that developed countries are trying to do. Then he goes on and says in the article:

> "If you study main international practices in this regard, you will find that China basically is in compliance with the international norm. The main purpose and methods of implementing our laws are basically the same."

Then he goes on to even say that the Bush Administration gained under the Patriot Act access to monitor Web sites and e-mail communications, the deployment of technology by the FBI to let agencies scrutinize huge volumes of e-mail traffic were examples of how the United States has taken legal steps to guard

against the spread of harmful information online. He says, "Clearly, any country's legal authorities closely monitor the spread of illegal information." One more final quote from him: "We have noted that the U.S. is doing a good job on this front."

Now, I alluded to the fact that I would like to see us have some oversight hearings and have a very open, robust discussion about what is the law, going and getting the Court approval and following current FISA law and all of that. We need to have that discussion ourselves so that we are speaking with one voice. How difficult is your job when your boss's words kind of come back to be used against you when you are trying to talk about freedom of information and privacy rights?

Mr. GROSS. Well, this has actually been an issue of longstanding. There are sometimes, as you have just read, recent examples that other governments tried to use, but we should always be mindful of the fact that ever since I have had my job now, for about 4½ years, other governments have said, well, this is all just basically a matter of line drawing. Everyone agrees there are certain things that there should not be on the Internet. We may draw our line differently than you draw your line, but it is all just line drawing.

I think that argument misses a very fundamental fact. It is one thing for democratic countries to go through the exercise of line drawing. It is something very different when nondemocratic governments seek to use the restriction of the free flow of information to keep themselves in power.

So we see there to be a fundamental difference, recognizing that reasonable people in democracies can draw different conclusions about what is or may not be appropriate in a particular circumstance, but there is a very fundamental difference that the sort of quotes that you just read, which I read as well, and I think many people did—they are not unique at all—fundamentally just miss the point, and it shows, I think, the gulf of difference in terms of approaches.

It would be a mistake for us to think this is a recent set of discussion points. Unfortunately, for us, these have been longstanding discussion points, and, again, it really goes to the question of how those decisions are made. Are they made in a democratic type of government situation? I think in all situations, governments should err on the side of allowing for the free flow of information, recognizing that the lines can be drawn differently where other types of governments draw the line very differently and find that restriction is their first choice, and liberalization is only done when there is a reason to do it.

Mr. SMITH OF NEW JERSEY. Ambassador Watson?

Ms. WATSON. Thank you, Mr. Chairman. This is a very, very interesting and telling discussion.

It was mentioned that there might be some consideration when looking at agreements between an American company doing business in China that we might start incorporating Internet protocol procedures. I would like a response from the two of you. If such is to be, what would you see, and how binding would you see these procedures when an American company decides to do business and relates to the government of that country, you know, here in this country you go into private arrangements that not necessarily the

government has to be involved in. But if we do such, what would you see, just kind of off the top of your heads, as procedures?

Mr. GROSS. Perhaps I will start and give my colleague more time to think of a good answer for your very good question.

I think, in the first instance, one of the things which we struggle with, which I know you all are struggling with as well, is the need for flexibility, particularly as technology changes. One of the things that makes this whole area very difficult is it is not static. It is extraordinarily dynamic, and, therefore, the issues are dynamic.

So, at the first instance, and one of the things I was so pleased as I was reviewing the comments made at the caucus a few days ago, was, I think, the general recognition that our first instinct should be to see if there are global best practices that can be established, and I do not mean like best practices but very substantial, very carefully worked out best practices that would have the sort of flexibility built into them to continue to evolve as these issues evolve, and only if that does not happen do we think that we should be stepping in to sort of try to manage that situation.

I think the problem here is, in many respects, the opportunities, which are the dynamic factors associated with it. So I think the protocol there, to use the term that you were using, is one of flexibility, and it also allows us, of course, to address some of the issues that other Members have raised as well, which is that this is not just a bilateral issue. This really is something that is multilateral in its nature. It is something that affects other governments, other companies from other countries as well. Reaching out in that global fashion allows us to do that in ways that we might not be able to do domestically.

Mr. KEITH. I would just add that, of course, there are multilateral channels for us to address these issues as well, and that is one approach.

Another approach is the bilateral one. The tool you refer to would be one of those in our bilateral kit bag, so to speak. It seems to me, in general, our success with the Chinese has been in promoting or supporting change. Our success has been in those areas where we can point to the Chinese interests and get them to recognize their own interests, and in some areas we have had less success than others.

But to the extent that we can show them that, to get to one of the Chairman's points earlier, the question of stability, the question of attracting foreign direct investment, the question of creating the infrastructure for doing business in China are all caught up in this. All involve China's own self-interest, and, over time, our goal, from the government's perspective, is to convey to the Chinese that creating an atmosphere in which their own interests are served is convergent with our approach, which is, of course, anchored in American interests.

One of the goals in this approach would be to show the Chinese why, in the long term, they ought to do this out of their own self-interest.

Ms. WATSON. I hope that as we preach to China or anywhere else in the world, we practice what we preach. You know, people watch everything we do. They have got this Internet ability. I understand, and you can comment on this, that the Chinese Government went

into the northern and western part of their country and identified 10,000 people with the highest IQs and sent them into technological institutes for training. So we are dealing with very gifted people looking at the use of communications and the Internet in the future, and I think our country has to take into consideration their flexibility, the way they think, and the wisdom that comes out of thousands and thousands and thousands of years of living on this planet.

I hear this discussion, and I am saying, you know, people are defending, shall I say, their freedoms, and people are also defending the tapping into other's conversations and gathering information. So there is a mixed message going out there. I do not know where this country stands. So that is why I raised the question, what you thought the procedure should be, and I heard one response, that there has to be flexibility, and there has to be what they feel is in their best interest, but it has to be made public and not shrouded in secrecy. There is a tendency for this Government of ours to shroud what it does in secrecy, so we cannot have it both ways.

The other thing I want to raise is, with respect to Yahoo! and MSN having provided information to Chinese authorities, to your knowledge, are they in violation of any applicable United States laws?

Mr. GROSS. Not to our knowledge, but we will leave that, I think, to others to discuss in more detail.

Ms. WATSON. Okay. So I think this would probably come up if we had such a task force, and I am really pleased that the Secretary of State has found it necessary to put such together. I commend that move because I think this is worthy of lots and lots of discussion and debate and not knee-jerk reactions. We really need to think it through.

We are dealing with the most populous nation on the globe with a long history. Ours is new, relatively, and so we have got to continue to have dialogue, and that is what bothers me about the way things are being done. We strike first and then want to discuss later. No. Before we make decisions that will impact on businesses in these United States as they relate to doing business in other countries, let us have thorough, complete, empirical kinds of evidence and dialogue based on that.

I think you might have responded to this question, but are there examples in other countries, say, in the Middle East, where services provided by United States Internet providers are circumscribed or monitored? Do you know?

Mr. GROSS. Yes. In fact, actually, in some respects, even the bigger problem there is the lack of the ability to compete in those markets themselves, but there are some very severe restrictions on access to information in many countries in the Middle East, and this has been a source of focus for us.

One place in which this got a lot of attention recently was Tunisia because it was the host government for the UN World Summit on the Information Society, and this was an area in which both are government and other governments as well and many NGOs and others were very outspoken about because of our strong commitment to ensuring the free flow of information.

Ms. WATSON. Thank you. Let me end by asking that you gentlemen and the others on the panel come back. We have a responsibility in this Congress to do oversight hearings. We do not do them as often as I feel are necessary.

I was the Ambassador to the Federated States of Micronesia, and I, underground, started a newspaper just to inform the people that we had a cholera epidemic and that they should know so that they will not practice high-risk behavior. Of course, we worked it out ourselves, but I would hope that our respective Committees would do more oversight, that you would come back to us as this task force develops and let us know of your thinking and where the State Department would be in relationship to these countries and in relationship to the governments that we are concerned about.

So I will ask the Chair to hold another one of these hearings down the line so we can know the progress being made, and with that, thank you very much, Mr. Chairman, for the time.

Mr. SMITH OF NEW JERSEY. The time of the gentlelady has expired.

I want to thank our first panelists for their expert witness and testimony and, above all, for the good work you do day in and day out on behalf of freedom, freedom of information, and human rights. Thank you so much for being here.

Mr. KEITH. Thank you, Mr. Chairman.

Mr. GROSS. Thank you, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. I would like to invite our second group of panelists to the witness table, beginning first with Mike Callahan, who was appointed Senior Vice President, General Counsel, and Secretary of Yahoo! in September 2003 after previously serving as Yahoo!'s Deputy General Counsel and Assistant Secretary. Mr. Callahan is responsible for the worldwide legal affairs and public policy of Yahoo!, as well as advising the company's management and board of directors on strategic and corporate governance matters. Prior to joining Yahoo!, Mr. Callahan was with Electronics for Imaging, Inc.

We will then hear from Mr. Jack Krumholtz, who is the Managing Director of Federal Government Affairs and Associate General Counsel in the Law and Corporate Affairs Department at Microsoft. Prior to joining Microsoft, Mr. Krumholtz was an attorney with a law firm in Washington, DC, where he practiced in the legislative and government relations area. Mr. Krumholtz serves on the Advisory Council to the Congressional Internet Caucus and the Software Division Board of the Information Technology Association of America.

We will then hear from Elliot Schrage, who is responsible for corporate communications and public affairs, which encompasses media relations, stakeholder outreach, and policy strategy for Google. Prior to joining Google, Elliot was the Bernard L. Schwarz Senior Fellow in Business and Foreign Policy at the New York-based Council on Foreign Relations and an advisor to several global corporations on issues of corporate social responsibility.

And, finally, we will hear from Mark Chandler, who is Senior Vice President, General Counsel, and Secretary of Cisco Systems. He was previously General Counsel of StrataCom, Inc., which Cisco acquired in 1996, and Vice President, Corporate Development, and

General Counsel of Maxtor Corporation, a Fortune 500 manufacturer of computer data storage devices. Mr. Chandler is also on the Advisory Council of the Woodrow Wilson International Center for Scholars.

If I could ask you gentlemen if you would not mind standing and taking an oath. You would raise your right arm.

[Witnesses sworn.]

Mr. SMITH OF NEW JERSEY. Let the record show that each of our witnesses answered in the affirmative, so if we could begin with Mr. Callahan and please proceed as you would like.

TESTIMONY OF MR. MICHAEL CALLAHAN, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, YAHOO! INC.

Mr. CALLAHAN. Thank you very much, Mr. Chairman, Chairmen Smith and Leach, Ranking Members Payne and Faleomavaega, and Members of the Subcommittees. I am Michael Callahan, Senior Vice President, General Counsel, and Secretary of Yahoo!. Thank you very much for the opportunity to testify before you today.

I would like to make three fundamental points. First, our principles. Since our founding in 1995, Yahoo! has been guided by beliefs deeply held by our founders and sustained by our employees. We believe the Internet can positively transform lives, societies, and economies. We believe the Internet is built on openness. We are committed to providing individuals with easy access to information. These beliefs apply in the United States. These beliefs also apply in China, where the Internet has grown exponentially over the past few years and has expanded opportunities for access to communications, commerce, and independent sources of information for more than 100 million Chinese citizens.

Second, the Shi Tao case. The facts of the Shi Tao case are distressing to our company, our employees, and our leadership. Let me state our view clearly and without equivocation: We condemn punishment of any activity internationally recognized as free expression, whether that punishment takes place in China or anywhere else in the world. We condemn it. Mr. Chairman, we have made our views known to the Chinese Government.

Third, this hearing. We commend you, Mr. Chairman, for holding this hearing. It allows these issues to be raised in a public forum. While we absolutely believe that companies have a responsibility to identify appropriate practices in each market where they do business, we also think there is a vital role for a government-to-government dialogue of the larger issues involved. In this regard, we applaud the direction of the Secretary of State in establishing a Global Internet Freedom Task Force.

We believe these issues are larger than any one company or any one industry. We all face the same struggle between American values and the laws we must obey. Yahoo! intends to be a leader in the discussion between U.S. companies and the U.S. Government. We appeal to the U.S. Government to do all it can to help us continue to provide beneficial services to Chinese citizens lawfully and in a way that is consistent with our shared values.

Allow me to clarify Yahoo!'s current role in China. In October of last year, Yahoo! formed a strategic, long-term partnership with Alibaba.com, a Chinese company, and merged our China business

with Alibaba.com. We do not have day-to-day operational control over Yahoo! China, but as a large equity investor, we have made clear our desire that Alibaba continue to apply rigorous standards in response to government demands for information about its users. I have personally discussed our views with senior management of Alibaba, as have other senior executives of Yahoo!.

Mr. Chairman, we believe information is power. We also believe that the Internet is a positive force in China. It has revolutionized information access, helps create more open societies, and accelerates the gradual evolution toward a more outward-looking Chinese society.

The Internet has grown exponentially in China in ways that have increased China's openness to the outside world. More than 110 million in China use the Internet, with more than 400 million search queries taking place very single day. That represents an increase of almost 1,600 percent over the last 3 years.

In my prepared testimony, I mention a couple of examples in which the Internet forced the Chinese Government to be more open and more transparent. Many recent public comments, including from a researcher at the Chinese Academy of Social Sciences and a former official from the China state media, have publicly recognized that the government cannot control the Internet.

Despite these extraordinary benefits, there are severe challenges for any company operating in China and especially those in the Internet, media, or telecommunications industries.

This brings us to the case of Shi Tao. The Shi Tao case raises profound questions about basic human rights. It is important to lay out the facts. When Yahoo! China in Beijing was required to provide information about a user, who we later learned was Shi Tao, we had no information about the identity of the user or the nature of the investigation. Indeed, we were unaware of the particular facts surrounding this case until the news story emerged.

Law enforcement agencies in China, in the United States, and elsewhere typically do not explain to information technology companies of other businesses why they demand specific information regarding certain individuals. In many cases, we do not know the real identity of these individuals for whom governments request information. Very often, our users may subscribe without using their real name to our service.

At the time the demand was made for information in this case, Yahoo! China was legally obligated to comply with the requirements of Chinese law enforcement. When we had operational control of Yahoo! China, we took steps to make sure that our Beijing operation would honor such demands only if they came from authorized law enforcement officers and only if the demand for information met rigorous standards establishing the legal validity of the demand.

When we receive a demand from law enforcement authorized under the law of the country in which we are operating, we must comply. Failure to comply in China could have subjected Yahoo! China and its employees to criminal charges, including imprisonment. Ultimately, American companies face a choice: Comply with Chinese laws or leave.

Mr. Chairman, we recognize this is not a time for business as usual. We are committing to the following. First, collective action. We will work with industry, government, academia, and NGOs to explore policies to guide industry practices in countries where content is treated more restrictively than in the United States and to promote the principles of freedom of speech and expression.

Second, compliance practices. We will continue to employ rigorous procedural protections under applicable laws in response to government requests for information, maintaining our commitment to user privacy and compliance with the law.

Third, information restrictions. Where a government requests that we restrict search results, we will do so if required by applicable law and only in a way that impacts the results as narrowly as possible. If we are required to restrict search results, we will strive to achieve maximum transparency to the user.

Fourth, government engagement. We will actively engage in an ongoing policy dialogue with governments with respect to the nature of the Internet and the free flow of information.

The strength of this industry and the power of our user base is formidable, to be sure, but we cannot do it alone. We will do everything we can to advance our commitments. Ultimately, the greatest leverage lies with the U.S. Government.

Mr. Chairman and Ranking Members, thank you for giving me the opportunity to appear before you.

[The prepared statement of Mr. Callahan follows:]

PREPARED STATEMENT OF MR. MICHAEL CALLAHAN, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, YAHOO! INC.

Chairmen Smith and Leach, Ranking Members Payne and Faleomavaega, and Members of the subcommittees, I am Michael Callahan, Senior Vice President, General Counsel and Secretary of Yahoo! Inc. Thank you very much for the opportunity to testify before you today.

I would like to make three fundamental points here today:

First, our principles. Since our founding in 1995, Yahoo! has been guided by beliefs deeply held by our founders and sustained by our employees. We believe the Internet can positively transform lives, societies, and economies. We believe the Internet is built on openness. We are committed to providing individuals with easy access to information. These beliefs apply in the United States. These beliefs also apply in China, where the Internet has grown exponentially over the past few years and has expanded opportunities for access to communications, commerce, and independent sources of information for more than 110 million Chinese citizens.

Second, the Shi Tao case. I will discuss this in more detail later in my testimony. The facts of the Shi Tao case are distressing to our company, our employees, and our leadership. Let me state our view clearly and without equivocation: we condemn punishment of any activity internationally recognized as free expression, whether that punishment takes place in China or anywhere else in the world. We have made our views clearly known to the Chinese government.

Third, this hearing. We commend you, Mr. Chairmen, for holding this hearing. It allows these issues to be raised in a public forum and provides an opportunity for companies such as those appearing here today to ask for the assistance of the U.S. government to help us address these critical issues. While we absolutely believe companies have a responsibility to identify appropriate practices in each market in which they do business, we also think there is a vital role for government-to-government discussion of the larger issues involved.

These issues are larger than any one company, or any one industry. We all face the same struggle between American values and the laws we must obey. Yahoo! intends to be a leader in the discussion between U.S. companies and the U.S. government. We appeal to the U.S. government to do all it can to help us provide beneficial services to Chinese citizens lawfully and in a way consistent with our shared values.

The Impact of the Internet In China

Before discussing these issues in detail, allow me to clarify Yahoo!'s current role in China. In October 2005, Yahoo! formed a long-term strategic partnership in China with Alibaba.com, a Chinese company. Under the agreements, Yahoo! merged our Yahoo! China business with Alibaba.com.

It is very important to note that Alibaba.com is the owner of the Yahoo! China businesses, and that as a strategic partner and investor, Yahoo!, which holds one of the four Alibaba.com board seats, does not have day-to-day operational control over the Yahoo! China division of Alibaba.com. The Alibaba.com management team runs the business; however, as a large equity investor, we have made clear our desire that Alibaba.com continue to apply rigorous standards in response to government demands for information about its users. I have personally discussed our views with senior management of Alibaba.com, as have other senior executives of Yahoo!.

Mr. Chairmen, we believe information is power. We also believe the Internet is a positive force in China. It has revolutionalized information access, helps create more open societies, and helps accelerate the gradual evolution toward a more outward-looking Chinese society.

The Internet has grown exponentially in China in ways that have increased China's openness to the outside world. More than 110 million people in China use the Internet. A growing Chinese middle class is benefiting from improved communication, technology, and independent sources of information. Online search, a core Yahoo! China service, is used by 87% of the online population in China, with more than 400 million search queries taking place every day. This represents an increase of almost 1600% over just the last three years. Unlike virtually any medium that has preceded it, the Internet allows users to access the information they want when they want it.

The number of people communicating with each other over the Internet has also increased dramatically. The number of active mailboxes has grown by 88% to 166 million, and those using instant messaging has risen to 87 million, doubling in just three years.

Let me give you a couple of examples of the power of the Internet in China. In November 2002, a new respiratory illness developed in southern China. This illness spread to other areas of China and in Asia. Initially, state media did not report widely on the outbreak, limiting access to information on SARS in China. However, word spread quickly through channels on the Internet, alerting people in China and around the world of the severity of the epidemic. The Internet forced the Chinese government to be more transparent and to vigorously attack the problem.

Another example is currently highlighted on the Human Rights Watch website. Human Rights Watch, with which we have consulted on these issues, tells the compelling story of how the Internet helped spread the word in China about the tragic death of a young college graduate named Sun Zhigang while in police custody. A storm of online protests led to the abolition of the law used to detain Mr. Sun. Human Rights Watch's website states, "[t]he Sun Zhigang case showed how Internet activists and journalists could mobilize an online uprising that produced real change." [1]

Experts in China and the United States agree on the liberalizing impact of the Internet in China. Please note the comments of a Chinese Academy of Social Sciences researcher in the *New York Times* last week. This expert stated, "At first, people might have thought it [the Internet] would be as easy to control as traditional media, but now they realize that's not the case." [2]

Finally, I would commend to you a 2002 report by the well-respected RAND Corporation that made an even bolder conclusion. It concluded that the Internet has allowed dissidents on the mainland to communicate with each other with greater ease and rapidity than ever before.[3]

But even with these extraordinary benefits, there are severe challenges for any company operating in China, and particularly for those in the Internet, media, or telecommunications industries. This Committee correctly highlights the fundamental conflict between the extraordinary powers of the Internet to expand opportunities for communication and access to information with the obligations of compa-

---

[1] Human Rights Watch, "Chinese Protest Online: The Case of Sun Zhigang," located at http://www.hrw.org/campaigns/china/beijing08/voices.htm.

[2] Howard W. French, "Despite Web Crackdown, Prevailing Winds Are Free," *New York Times*, Feb. 9, 2006.

[3] Michael S. Chase and James C. Mulvenon, *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies*, RAND Corporation monograph, 2002, page 3.

nies doing business in China to comply with laws that may have consequences inconsistent with our values. This brings us to the case of Shi Tao.

The Facts Surrounding the Shi Tao Case

The Shi Tao case raises profound and troubling questions about basic human rights. Nevertheless, it is important to lay out the facts. When Yahoo! China in Beijing was required to provide information about the user, who we later learned was Shi Tao, we had no information about the nature of the investigation. Indeed, we were unaware of the particular facts surrounding the case until the news story emerged. Law enforcement agencies in China, the United States, and elsewhere typically do not explain to information technology companies or other businesses why they demand specific information regarding certain individuals. In many cases, Yahoo! does not know the real identity of individuals for whom governments request information, as very often our users subscribe to our services without using their real names.

At the time the demand was made for information in this case, Yahoo! China was legally obligated to comply with the requirements of Chinese law enforcement. When we had operational control of Yahoo! China, we took steps to make clear our Beijing operation would honor such instructions only if they came through authorized law enforcement officers and only if the demand for information met rigorous standards establishing the legal validity of the demand.

When we receive a demand from law enforcement authorized under the law of the country in which we operate, we must comply. This is a real example of why this issue is bigger than any one company and any one industry. All companies must respond in the same way. When a foreign telecommunications company operating in the United States receives an order from U.S. law enforcement, it must comply. Failure to comply in China could have subjected Yahoo! China and its employees to criminal charges, including imprisonment. Ultimately, U.S. companies in China face a choice: comply with Chinese law, or leave.

Let me take this opportunity to correct inaccurate reports that Yahoo! Hong Kong gave information to the Chinese government. This is absolutely untrue. Yahoo! Hong Kong was not involved in any disclosure of information about Mr. Shi to the Chinese government. In this case, the Chinese government ordered Yahoo! China to provide user information, and Yahoo! China complied with Chinese law. To be clear—Yahoo! China and Yahoo! Hong Kong have always operated independently of one another. There was not then, nor is there today, any exchange of user information between Yahoo! Hong Kong and Yahoo! China.

Next Steps

Yahoo! continues to believe the continued presence and growth of the Internet in China empowers its citizens and will help advance Chinese society. The alternative would be for these services to leave China—a move we believe would impede Chinese citizens' ability to communicate and access independent sources of information. But we recognize this cannot be a time for business as usual.

As part of our ongoing commitment to preserving the open availability of the Internet around the world, we are committing to the following:

- *Collective Action:* We will work with industry, government, academia and NGOs to explore policies to guide industry practices in countries where content is treated more restrictively than in the United States and to promote the principles of freedom of speech and expression.
- *Compliance Practices:* We will continue to employ rigorous procedural protections under applicable laws in response to government requests for information, maintaining our commitment to user privacy and compliance with the law.
- *Information Restrictions:* Where a government requests that we restrict search results, we will do so if required by applicable law and only in a way that impacts the results as narrowly as possible. If we are required to restrict search results, we will strive to achieve maximum transparency to the user.
- *Government Engagement:* We will actively engage in ongoing policy dialogue with governments with respect to the nature of the Internet and the free flow of information.

Let me make one final comment about the role of the U.S. government. We urge the U.S. government to take a leadership role on a government-to-government basis. The Internet industry in the United States, including the companies appearing before you today, have changed the way the world communicates, searches for, discovers, and shares information. No other medium in history has the potential to effect such great change so rapidly. We operate businesses that transcend boundaries,

in a world of countries and borders. The strength of this industry and the power of our user base is formidable to be sure. But, we cannot do it alone. We will do everything we can to advance these principles. Ultimately, the greatest leverage lies with the U.S. government.

Chairmen Smith and Leach, Ranking Members Payne and Faleomavaega, and Members of the subcommittees, thank you for giving me the opportunity to appear before you. We welcome this chance to have a frank and open dialogue about this important issue. We are grateful for your willingness to understand the difficult challenges we face, and to help us as we work together to protect the ability of the citizens of the world to access communication, commerce, and independent sources of information. I would be happy to answer your questions.

Mr. SMITH OF NEW JERSEY. Mr. Callahan, thank you so very much.

Mr. Krumholtz?

TESTIMONY OF MR. JACK KRUMHOLTZ, MANAGING DIRECTOR OF FEDERAL GOVERNMENT AFFAIRS AND ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION

Mr. KRUMHOLTZ. Chairman Smith, Ranking Member Payne, Chairman Leach, Ranking Member Faleomavaega, and Members of the Subcommittee, Microsoft welcomes the opportunity to address the issues surrounding Internet-based services in China. We are deeply concerned about recent events that have prompted widespread public concern over matters of individual security and government control of Internet content in that country, and we are actively seeking ways of reducing risks to individual users while maximizing the availability of information and opinion through these services.

My written testimony elaborates on the challenges companies like Microsoft face in providing Internet services in countries whose laws and free speech protections do not mirror our own. In the interest of time, I would like to focus my remarks on three main points.

First, Internet services like Microsoft MSN Spaces which host personal Web sites or "blogs" are having a major positive impact in China despite the effort by various agencies of the Chinese Government to control certain kinds of political content. In just the past few years, we have seen repeated examples in China of official responses to domestic developments that have been shaped for the better because of information provided and opinions expressed over the Internet. Most prominent have been reports about the government's handling of health issues, such as SARS and Avian flu, many of them circulated by personal Web sites.

While there are competing blog services offered by some Chinese companies, Microsoft's service, which was launched less than 9 months ago, is now the largest, with more than 3.5 million users. The overwhelming majority of Internet-based communications and search are not politically oriented, but a survey of Chinese Internet users found that 48 percent believe that by going online, the Chinese will learn more about politics, and 60 percent believe that the Internet will provide more opportunities for criticizing government.

Mr. Chairman, this is the powerful reality of the Internet in China today. The Internet has already transformed the economic, cultural, and political landscape of China. It is vital that companies, particularly American companies, with the widest array of

communications and information services, continue to offer services there.

Second, Microsoft is committed to working with governments, industry, and other stakeholders to protect the best interests of our customers, but enacting legislation that effectively forces us to withdraw from China would be counterproductive. We recognize from conversations with Members and staff of these Subcommittees that you have strong concerns that American companies somehow embrace Chinese censorship of the Internet. Let me assure you that that is not the case. Microsoft is deeply troubled by the restrictive regulations we operate under in China. We comply with them only to the extent required by law. However, to suggest that we can resist or defy these regulations assumes a much different reality than the one we deal with in China on a regular basis.

While we are actively exploring how best to protect the interests of our users under these circumstances, we do not have the influence or leverage to pressure the Chinese into changing their regulations or refraining from enforcing them. At the same time, we are not suggesting that compliance with local law is a matter of deferring reflexively to local authorities or endorsing any specific policy or ideology.

The simple fact is that there is not a government in the world, including the United States, which would accept the proposition that companies can set their own terms of operation in defiance of local law. Moreover, there are Chinese competitors for our services, competitors who would like nothing better than to see us forced to stop offering them in China.

Ultimately, we must ask ourselves, will the Chinese citizens be better off without access to our services?

Third, the issues we face are global in scope. It is essential that the U.S. Government play an active role in building a consensus for the widest possible availability of information over the Internet. The Internet raises issues of legitimate governmental concern, including matters of privacy, child safety, and national security, but authorities around the world have made different judgments about the standards appropriate to their cultures and national circumstances. The Chinese effort to manage content on the Internet is just the most troubling of these fundamental differences.

It is, therefore, the responsibility of governments, with the active leadership of the United States, to seek to reduce or reconcile these differences in order to protect the value and power of the Internet on a global basis. Here again, companies like Microsoft can play an active role in supporting such efforts to promote a deeper consensus across many nations.

We, therefore, welcome yesterday's announcement by the Secretary of State creating the Global Internet Freedom Task Force and look forward and are committed to working with that group.

What Microsoft will continue to do is what we do best: Provide the technologies and services that enable individuals and organizations to harness the power of the Internet for their own purposes. We think that the trend of history will continue to come down on the side of openness and transparency, as it has increasingly been doing in China and as it will ultimately do everywhere else.

Thank you for the opportunity to discuss these issues with the Subcommittees, and we look forward to working with you on this important issue.

[The prepared statement of Mr. Krumholtz follows:]

PREPARED STATEMENT OF MR. JACK KRUMHOLTZ, MANAGING DIRECTOR OF FEDERAL GOVERNMENT AFFAIRS AND ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION

Microsoft welcomes the opportunity to address the issues surrounding Internet-based services in China. We are deeply concerned about recent events that have prompted widespread public attention to issues of individual security and government control of Internet content in that country. And we are actively seeking ways of maximizing the availability of information and opinion through these services while reducing the risks to individual users.

Microsoft believes that issues of Internet content and customer security go to the heart of our values as a company. The Internet should be fostered and protected as a worldwide vehicle for reliable information and communications, personal expression, innovation and economic development. Microsoft seeks to advance that objective by providing services such as our free Hotmail email service, and free personal websites or "blogs" on the MSN Spaces service, as well as reliable access through the MSN portal to the millions of websites that have made the Internet such a magnet for education, commerce, entertainment, and, increasingly, for personal communications and expression.

Global Dimensions

At the same time, the Internet raises issues that often justify government attention, especially on matters of individual privacy, law enforcement, and national security. On some of these issues, governments around the world have made differing judgments about the legal standards and policy trade-offs appropriate to their own cultures and national circumstances—in many cases issuing regulations or codes of conduct that define limits on permissible content and prescribe procedures for identifying authorship. While the exercise of governmental responsibilities is usually well-intentioned and limited, it is critically important for the future of the Internet—and thereby for the future of the global community and economy as a whole—that all governments address these issues with deliberation and restraint. Legal and regulatory steps should be taken only with the utmost attention to their wider consequences—including the impact on individuals, enterprises and societies far beyond the borders of the initiating countries. International meetings and bilateral consultations may increasingly help to promote the consistency of national actions and to maximize the openness, security and reliability of the Internet platform. Indeed, the greatest influence over time on national policies affecting the Internet, including those of the Chinese government, is likely to come from a combination of bilateral and multilateral processes of consultation and consensus-building. But the global consultative process is only just beginning to unfold.

In this regard, the U.S. government has a particularly important role to play. As the leading nation in the development and enhancement of the Internet, the United States has a special responsibility to engage in shaping the political context that will keep it flourishing responsibly. For that reason, the United States should intensify its vital leadership on these issues and initiate discussions with other governments—both bilateral and multilateral—to address restrictions on Internet content that might otherwise create major impediments to the utility of the medium and present unnecessary risks to individual users.

The private sector also has a vital role to play. While retaining its leading role in developing the technologies and standards that protect Internet security and reliability, industry should advocate policies and principles that maximize the value of the Internet for individual users, including basic protections for freedom of expression, commercial integrity and the reliability of information. We have initiated consultations with the companies at this hearing and others to consider the kinds of principles that would advance these values effectively on an industry basis. But, in the end, the legal framework in any particular jurisdiction is not one that private companies are in a position to define for ourselves. National law and policy set parameters in every country in which we do business, and private companies are required to give them due deference as a condition of engaging in business there.

That does not mean that compliance with local law is a matter of deferring reflexively to local authorities or endorsing any specific policy or ideology. Restrictions on content should involve ongoing consultations in which the objective of private operators is to protect the integrity of their services and the privacy of their customers.

Where the safety and security of individuals is at stake, it is incumbent on both governments and private companies to assure that requests for customer information in particular are subject to the highest available standards of legal process. When that information is not maintained in the country concerned, such requests necessarily invoke international agreements that require established government-to-government procedures. When it is maintained in the United States, private operators clearly must comply with applicable U.S. laws protecting on-line privacy, such as the Electronic Communications Privacy Act (ECPA). In addition, Microsoft will seek to provide appropriate notice and transparency to our customers about the standards that will be applied to their communications and the risks they may run if those standards are violated.

Let me be clear on one point: Microsoft will continually review the overall value of our services in any particular country and the conditions created by government policies and practices. If we conclude that those practices undercut or completely compromise the value to customers of our services in that jurisdiction, we will consider withdrawing those services until such conditions improve. But we must always keep squarely in mind whose interests would be best served by such a withdrawal. Will the citizens of that country be better off without access to our services, or will their absence just vindicate those who see our presence in the country as threatening to their official or commercial interests?

China as a Special Case

Microsoft is keenly aware that China presents a special case. Various agencies of the Chinese government are engaged in a substantial effort to manage the kinds of information available to Chinese citizens through the mass media. This effort includes specific regulations restricting the publication on the Internet of news-related content related to "current events news information, reporting and commentary relating to politics, economics, military affairs, foreign affairs, and social and public affairs, as well as reporting and commentary relating to fast-breaking social events." These regulations allow government authorities to restrict content for any of a number of reasons ranging from "harming the honor or the interests of the nation" to "disrupting the solidarity of peoples" to "disrupting national policies on religion, propagating evil cults and feudal superstitions" and "spreading rumors, disturbing social order, or disrupting social stability."[1] And these regulations encompass the kinds of Internet-based services provided by Microsoft's MSN division. The Chinese government's approach on these matters is well documented in a Report issued just this month by the well-respected NGO Freedom House.[2]

Yet, despite those efforts and the serious consequences for individuals who get caught up in the censorship process, the Internet has already transformed the economic, cultural and political landscape of China. In particular, it has had an enormous impact in increasing public access to information. To quote the Freedom House Report:

> "While the state has expended considerable effort to limit Chinese access to web pages deemed politically subversive, many users find ways to access blocked Internet sites by using proxies or anti-blocking software. The Internet has increased the speed and convenience of accessing information and decreased the financial costs of interpersonal communication . . ."

This is the powerful reality in China that we must not lose sight of in our concern for the worst cases of recent times. One recent independent survey of Chinese Internet users found that "48% percent of Internet users believe that by going on line the Chinese will learn more about politics, and *60% of users believe the Internet will provide more opportunities for criticizing the government."* [Emphasis added.][3]

As described in a New York Times report last week from Shanghai, the Internet offers the best opportunity for ordinary citizens in China to communicate their own observations and opinions and to report the facts about important local events.[4] Just in the past few years, there have been repeated examples in China of the ways in which official responses to domestic events have been affected by the availability of information and opinions communicated over the Internet. Most prominent have

---

[1] See the Rules on the Administration of Internet News Information Services, available on-line at http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

[2] Ashley Esarey, "Speak No Evil: Mass Media Control in Contemporary China," A Freedom House Special Report, February 2006, at page 11.

[3] "Surveying Internet Usage and Impact in Five Chinese Cities" by Guo Liang, Researdch Center for Social Development, Chinese Academy of Social Sciences, November 17, 2005, at page 97. (Sponsored by the Markle Foundation. See www.markle.org)

[4] "Despite Web Crackdown, Prevailing Winds Are Free," Letter from China by Howard French, NY Times,, February 9, 2006, at page A4.

been reports and commentary about the handling of health issues, such as SARS, Avian flu, HIV/AIDS and water contamination. They demonstrate the important role played by the kinds of services that companies like Microsoft provide over the Internet. Since its introduction in China last May, our MSN Spaces blogging service has attracted more than three and a half million users and over fifteen million unique readers, making it the #1 such service in China. As our General Counsel, Brad Smith, noted in reviewing our policies on these services:

> We think that blogging and similar tools are powerful vehicles for economic development and for creativity and free expression. . . . We believe that it's better to make these tools available than not.

Therefore, based on grounds of human rights and freedom of expression alone, Microsoft believes that we should continue to provide our Internet-enabled services in China. That is a judgment that we will continue to evaluate over time, drawing on the best advice we can get, including the opinions of the Members of Congress who follow these issues in China with great interest. If, on the other hand, the outcome of these hearings is to make it impossible for us to continue these services in China—either because of conditions imposed by our government, or because of further actions on the part of the Chinese government—we believe that the Chinese people would be the principal losers—being denied an important avenue of communication and expression.

Microsoft Concerns

Let there be no misunderstanding about the values that underlie Microsoft's decisions on this matter. Our people—from the senior management of the company to the more than 60,000 employees all over the world, including more than 2500 in China itself—care deeply about the impact of our services on the people we serve. We are actively reviewing all of our policies and practices to identify the best ways to protect customers, while providing the widest possible array of information sources.

The example that has received the most attention to our services in China involved the removal of a well-known blogging site on MSN Spaces authored under the pseudonym of "Michael Anti" at the request of the Chinese government. The details of that case have been carefully reviewed, and although we do not think we could have changed the Chinese government's determination to block this particular site, we regret having to do so and have since clarified the manner in which we will deal with similar requests in the future. Those policies seek to assure three things:

First, explicit standards for protecting content access: Microsoft will remove access to blog content only when it receives a legally binding notice from the government indicating that the material violates local laws, or if the content violates MSN's terms of use.

Second, maintaining global access: Microsoft will remove access to content only in the country issuing the order. When blog content is blocked due to restrictions based on local laws, the rest of the world will continue to have access. This is a new capability Microsoft is implementing in the MSN Spaces infrastructure.

Third, transparent user notification: When local laws require the company to block access to certain content, Microsoft will ensure that users know why that content was blocked, by notifying them that access has been limited due to a government restriction.

Our ongoing reviews may result in other changes of policy as we continue to examine our options and seek the input of a broad array of experts. In addition to active discussions within the industry and with the Executive branch, we have been meeting with NGO's focused on issues of human rights in China and will continue those discussions. We are seeking the advice of recognized experts on China to better understand the dynamics and trends affecting the issues we are addressing here. And we will continue to discuss these issues with Members of Congress, including testimony before appropriate Committees such as this one.

Industry Influence

Finally, let me address the suggestion that Microsoft alone, or in collaboration with other companies in our industry, should be able to change the standards enforced by the Chinese government—or alternatively, to negotiate the manner in which we choose to comply with those standards. Some commentators assert that we are in a position to temper or delay our degree of compliance with Chinese law and criminal process without losing our license to do business in China. Some have even suggested that we have not tried to pressure the Chinese government in this regard because we seek to curry favor for commercial reasons. These arguments ig-

nore the basic realities of doing business, not only in China, but in most other countries.

Indeed, witnesses at the Congressional Human Rights Caucus two weeks ago suggested or implied that private companies should never provide information to governments about the identity of customers or agree to any sorts of restrictions on Internet content. But the simple fact is that there is not a government in the world, including our own, which would accept such an assertion by a private company seeking to do business within their jurisdiction. Indeed, it is a well-established principle of international jurisdiction that global Internet companies have to follow the law in the countries where they provide services to local citizens, even when those laws are different from those in their country of origin.[5] Taking the contrary position in defiance of government directives would be tantamount to inviting sanctions—up to and including the prosecution of our employees, the termination of our services in-country and even exclusion of the company from doing business in the country entirely.

When pressed on this point, most observers would no doubt concede that there are circumstances—such as instances of kidnapping, child abuse, or cyber-attack—when the apprehension of serious criminals justifies cooperation with law enforcement authorities even in authoritarian societies—so long as law enforcement is not used as a pretext for political repression. Yet in practice, when companies face law enforcement requests of this kind, there is little room to question the motivations or and second-guess the judgments made by officials in these cases.

In the end, the issue comes back to a difficult judgment of the risks and benefits of these powerful technologies, not just in China, but in a wide range of societies where cultural and political values may clash with standards of openness and free expression. Microsoft cannot substitute itself for national authorities in making the ultimate decisions on such issues. What Microsoft will do is provide the technologies and services that enable individuals and organizations to harness the power of the Internet for their own purposes—if allowed to do so. And we will continue to advocate that people should have the maximum opportunity to use these technologies in exercising those decisions for themselves.

We think that the trend of history and the impact of technology will continue to come down on the side of greater openness and transparency—as it has in China, and as it is likely to do elsewhere. As our Chairman, Bill Gates, said recently in answer to a question about Internet censorship:

> *"You may be able to take a very visible Web site and say that something shouldn't be there, but if there is a desire by the population to know something, it is going to get out."*

Thank you for this opportunity to address the Subcommittees on these important matters.

Mr. SMITH OF NEW JERSEY. Thank you, Mr. Krumholtz.

Mr. Schrage?

TESTIMONY OF MR. ELLIOT SCHRAGE, VICE PRESIDENT FOR CORPORATE COMMUNICATIONS AND PUBLIC AFFAIRS, GOOGLE, INC.

Mr. SCHRAGE. Chairman Leach, Chairman Smith, Ranking Members Payne and Faleomavaega, and Members of the Committee, my name is Elliot Schrage, and I am the Vice President of global communications and public affairs at Google. I have submitted my full

---

[5] Indeed, even in the United States, both federal and state authorities have prosecuted those involved in offshore gaming activities despite the fact that the online casinos are located in jurisdiction in which the activities are legal. See, e.g., *Vacco v. World Interactive Gaming Corporation*, 714 N.Y.S.2d 844 (N.Y. Sup. Ct. 1999) (offshore Internet gambling operation held to violate federal laws and the state penal code). The court described the central issue as "whether the State of New York can enjoin a foreign corporation legally licensed to operate a casino offshore from offering gambling to Internet users in New York." It decided the state could do so because of the "deep-rooted policy of the state against unauthorized gambling." See also *In re Grand Jury Proceeding, US v. Bank of nova Scotia*, 691 F.2d 1384 (11th Cir. 1982) (affirming a district court decision holding the Bank of Nova Scotia in civil contempt for failing to comply with an order of the court enforcing a grand jury subpoena requiring it to produce documents in violation of Bahamian bank secrecy laws "even though the very fact of disclosure may subject the Bank to criminal sanctions by a foreign sovereign").

testimony for the record and will be very brief with my oral testimony.

What I would like to do is provide a little context and then just make a few points. Google was founded in 1998 with a business mission to organize the world's information and make it universally accessible and useful. For almost 6 years, we have been offering a Chinese language service that is unfiltered and uncensored for all users worldwide.

Since at least 2002, however, our users in China have experienced increasingly difficult, severe problems, indeed, accessing our service. As a result, we faced a difficult choice: Compromise our mission by failing to serve our users in China or compromise our mission by entering China and complying with Chinese laws that require us to censor search results.

Mr. Chairman, in an imperfect world, we had to make an imperfect choice. Based on what we know today and what we see in China, we believe our decision to launch the google.cn service, in addition to our google.com service, is a reasonable one, better for Chinese users and better for Google.

As I said, there are four points about the decision that I would like to highlight today.

First—our decision to create a presence, any presence, inside of China was a difficult one. Self-censorship, like that which we are now required to perform in China, is something that conflicts deeply with our core principles. We recognize the conflict and the inconsistency. We respect the opinions of those, including several Members of this Committee, who disagree with the decision that we have taken. But how did we reach our decision?

Point number two—we reached our decision by balancing three commitments: First, our commitment to user interests, our commitment to access to information, and our commitment to responding to local conditions. Our business commitment is to satisfy the interests of our users in China, to offer them great search product, speed, reliability, and, yes, privacy and confidentiality of their search results and information. That is how we built a successful business in the United States, and that is how we plan to build that business around the world. Second is our conviction that expanding access to information will make our world a better, more informed, and freer place. And, third, our need to be responsive to local conditions. In most countries, this, frankly, is not a challenge, but in China it most certainly is. Balancing these three interests, we have determined that we can do the most for our users and do more to expand access to information if we accept the censorship restrictions required by Chinese law.

So, point three—what are we offering in China? What we have done inside China is to offer a new site, an additional site, google.cn, which is a complement to our google.com service. We have offered google.cn as a search Web site inside China for Chinese users. The new service will have significant advantages over its local competitors, we believe. It will be faster, more reliable, with more and better search results for all but a handful of, yes, politically sensitive search requests. We are not happy about it, but that is the requirements. At the same time, google.cn has crucial protections for our users. We will provide them disclosure when we

are filtering. We will protect their privacy and confidentiality, and for those reasons who want to seek unfiltered results, we will continue to make the unfiltered results available through google.com.

The last point is—we are new to this. It is not appropriate to say that we are proud of our decision. It is just too early to say that. Our hope is that the decision will prove to be the right one. If, over time, we are not able to achieve our objectives to continue to balance those interests in China, we will not hesitate to reconsider doing business in that market.

Finally, I would like to offer two suggestions for the industry and for this Committee. First, absolutely, there is a role for joint industry action. We certainly can and should come up with common principles around such issues as disclosure and transparency, perhaps public reporting of the kinds of censorship requests we get, as well as best practices for protecting user data.

And certainly also, finally, there is a role for government. We do need your help, and you can help us. For example, censorship should become a central part of the bilateral and multilateral trade agenda. We could, for example, treat censorship as a barrier to trade and raise that issue in appropriate fora.

I look forward to your questions, and thank you again for this opportunity.

[The prepared statement of Mr. Schrage follows:]

Testimony of Google Inc.

Before the
Subcommittee on Asia and the Pacific, and the
Subcommittee on Africa, Global Human Rights, and International Operations
Committee on International Relations
United States House of Representatives
February 15, 2006

Elliot Schrage
Vice President, Global Communications and Public Affairs
Google Inc.

My name is Elliot Schrage and I am the vice president for global communications and public affairs at Google. My role is to help shape and explain the decisions Google makes as a company in its efforts to provide global access to information as quickly, conveniently, usefully, and comprehensively as possible.

I'm here today to answer any and all questions you might have about how we are attempting to do business in China. I certainly don't – my colleagues certainly don't – expect everyone to agree with our decision to launch a new service inside this challenging, complex, promising market. I hope my testimony will help explain how we came to our decision, what we're seeking to accomplish, and how we're seeking to accomplish it.

Introduction

At the outset, I want to acknowledge what I hope is obvious: Figuring out how to deal with China has been a difficult exercise for Google. The requirements of doing business in China include self-censorship – something that runs counter to Google's most basic values and commitments as a company. Despite that, we made a decision to launch a new product for China – Google.cn – that respects the content restrictions imposed by Chinese laws and regulations. Understandably, many are puzzled or upset by our decision. But our decision was based on a judgment that Google.cn will make a meaningful – though imperfect – contribution to the overall expansion of access to information in China.

Until a few weeks ago, Google has been serving Chinese Internet users the same way we serve all Internet users worldwide since the company was founded in 1999. Though we had no operations or employees in China, we were able to provide a Chinese-language version of Google.com that, thanks to the global nature of the Internet, could easily be reached by users inside China. In 2002, we started to learn that Google was sporadically unavailable to Chinese users. In the fall of that year, we awoke one morning to emails from Google users in China informing us that our service was completely unavailable. We faced a choice at that point: hold fast to our commitment

to free speech (and risk a long-term cut-off from our Chinese users), or compromise our principles by entering the Chinese market directly and subjecting ourselves to Chinese laws and regulations. We stood by our principles, which turned out to be a good choice, as access to Google.com was largely restored within about two weeks.

However, we soon discovered new problems. Many queries, especially politically sensitive queries, were not making it through to Google's servers. And access became often slow and unreliable, meaning that our service in China was not something we felt proud of. Even though we weren't doing any self-censorship, our results were being filtered anyway, and our service was being actively degraded on top of that. Indeed, at some times users were even being redirected to local Chinese search engines Nevertheless, we continued to offer our service from outside China while other Internet companies were entering China and building operations there.

A bit more than a year ago, we decided to take a serious look at China and re-assess whether our approach there was the best strategy. We spent a lot of time talking to Chinese Internet experts and users, scholars and academics inside and outside China, respected "China hands," human rights groups and activists, government officials, business leaders, as well as our own Chinese employees. From those discussions, we reached the conclusion that perhaps we had been taking the wrong path. Our search results were being filtered; our service was being crippled; our users were flocking to local Chinese alternatives; and, ultimately, Chinese Internet users had less access to information than they would have had.

Let me dig a bit deeper into the analytic framework we developed for China. Google's objective is to make the world's information accessible to everyone, everywhere, all the time. It is a mission that expresses two fundamental commitments:

> (a) First, our business commitment to satisfy the ***interests of users***, and by doing so to build a leading company in a highly competitive industry; and
> (b) Second, our policy conviction that ***expanding access*** to information to anyone who wants it will make our world a better, more informed, and freer place.

Some governments impose restrictions that make our mission difficult to achieve, and this is what we have encountered in China. In such a situation, we have to add to the balance a third fundamental commitment:

> (c) Be responsive to ***local conditions***.

So with that framework in mind, we decided to try a different path, a path rooted in the very pragmatic calculation that we could provide more access to more information to more Chinese citizens more reliably by offering a new service – Google.cn – that, though subject to Chinese self-censorship requirements, would have some significant advantages. Above all, it would be faster and more reliable, and would provide more and better search results for all but a handful of politically sensitive subjects. We also developed several elements that distinguish our service in China, including:

- Disclosure to users -- We will give notification to Chinese users whenever search results have been removed.
- Protection of user privacy -- We will not maintain on Chinese soil any services, like email, that involve personal or confidential data. This means that we will not, for example, host Gmail or Blogger, our email and blogging tools, in China.
- Continued availability of Google.com -- We will not terminate the availability of our unfiltered Chinese-language Google.com service.

Many, if not most, of you here know that one of Google's corporate mantras is "Don't be evil." Some of our critics – and even a few of our friends – think that phrase arrogant, or naïve or both. It's not. It's an admonition that reminds us to consider the moral and ethical implications of every single business decision we make.

We believe that our current approach to China is consistent with this mantra. Our hope is that our mix of measures, though far from our ideal, would accomplish more for Chinese citizens' access to information than the alternative. We don't pretend that this is the single "right" answer to the dilemma faced by information companies in China, but rather a reasonable approach that seems likely to bring our users greater access to more information than any other search engine in China. And by serving our users better, we hope it will be good for our business, too, over the long run.

To be clear, these are not easy, black-and-white issues. As our co-founder Sergey Brin has said, we understand and respect the perspective of people who disagree with our decision; indeed, we recognize that the opposing point of view is a reasonable one to hold. Nonetheless, in a situation where there are only imperfect options, we think we have made a reasonable choice. It's a choice that has generated enormous attention – vastly more, indeed, than our earlier decisions not to cross the line of self-censorship. We hope that the ensuing dialogue will lead to productive collaboration among businesses and governments to further our shared aim of expanding access to information worldwide.

We think we have made a reasonable decision, though we cannot be sure it will ultimately be proven to be the best one. With the announcement of our launch of Google.cn, we've begun a process that we hope will better serve our Chinese users. We also hope that we will be able to add new services, if circumstances permit. We are also aware that, for any number of reasons, this may not come to pass. Looking ahead, we will carefully monitor conditions in China, including new laws and other restrictions on our services. If we determine that we are unable to achieve the objectives I've outlined above, we will not hesitate to reconsider our approach to China.

In the remainder of my written testimony below, I set forth the situation in China as we see it, the debate over the options we confronted, the substance of what Google has decided to do there, the reasoning behind that decision, and some ideas for both industry and governmental actions that could make a useful contribution to the objective of expanding access to information in every corner of the globe.

The Big Picture: The Internet is Transforming China

The backdrop to Google's decision to launch Google.cn is the explosive growth of the Internet in China. To put it simply, the Internet is transforming China for the better. And the weight of the evidence suggests that the Internet is accelerating and deepening these positive trends, even in an imperfect environment.

Viewed broadly, information and communication technology – including the Internet, email, instant messaging, web logs, bulletin boards, podcasts, peer-to-peer applications, streaming audio and video, mobile telephones, SMS text messages, MMS photo-sharing, and so on – has brought Chinese citizens a greater ability to read, discuss, publish and communicate about a wider range of topics, events, and issues than ever before.

There are currently more than 105 million Internet users in China.[1] Nearly half of them have access to broadband connections – an increase of 41% since 2003.[2] Even so, Internet deployment in China is at a very early stage, reaching only about 8% of the population.[3] Among those under 24 years of age, more than 80% are Internet users.[4] By 2010, China will have more than 250 million Internet users.[5] And already, there are more than 350 million mobile phones, a number growing by roughly 57 million annually.[6]

A recent and well-respected study by researchers at the Chinese Academy of Social Science (CASS) documents some interesting, and perhaps surprising, findings about the views of Chinese Internet users:[7]

- Most Chinese Internet users believe that the Internet is changing politics in China. Internet users tend to agree that it will increase political transparency and expand discourse: 63% believe that citizens will learn more about politics by going online, 54% of users believe the Internet provides more opportunities for criticizing the government, and 45% believe that the Internet provides more opportunities to express political views.
- Large majorities of Chinese believe that certain kinds of Internet content, including pornography and violence, should be controlled. However, only 7.6% believe that political content on the Internet should be controlled.
- By a 10:1 margin, Chinese Internet users believe that the Internet will make the world a better, rather than worse, place.

---

[1] "China Online Search Market Survey Report," China Network Information Center (CNNIC) (August 2005) ("CNNIC Search Engine Study").
[2] Guo Liang, "Surveying Internet Usage and Impact in Five Chinese Cities," Research Center for Social Development, Chinese Academy of Social Sciences (November 2005) ("the CASS Internet Survey"), at iii. The CASS Internet Survey is a statistically rigorous survey of Internet users in Beijing, Shanghai, Guangzhou, Chengdu, and Changsha.
[3] Id.
[4] Id., at iv.
[5] "15th Statistic Survey Report on the Internet Development in China," China Network Information Center (CNNIC) (2005).
[6] From statistics published by China's Ministry of Information Industry.
[7] CASS Internet Survey., at iv-ix, 93-100.

Based on its results, the CASS Internet Survey concludes that "the political impact of the Internet is more significant than it is in other countries. The impact can be seen not only in the relationship between government and citizens but also among people who share similar political interests. Thus, we can predict that as Internet becomes more popular in China, the impact on politics will be stronger."[8]

The Problem: Access to Google in China is Slow and Unreliable

Since 2000, Google has been offering a Chinese-language version of Google.com, designed to make Google just as easy, intuitive, and useful to Chinese-speaking users worldwide as it is for speakers of English.

Within China, however, Google.com has proven to be both slow and unreliable. Indeed, Google's users in China struggle with a service that is often unavailable. According to our measurements, Google.com appears to be unreachable around 10% of the time. Even when Chinese users can get to Google.com, the website is slow (sometimes painfully so, and nearly always slower than our local competitors), and sometimes produces results that, when clicked on, stall out the user's browser. The net result is a bad user experience for those in China.

The cause of the slowness and unreliability appears to be, in large measure, the extensive filtering performed by China's licensed Internet Service Providers (ISPs). China's laws, regulations, and policies against illegal information apply not only to the Internet content providers, but also to the ISPs. China has nine licensed international gateway data carriers, and many hundreds of smaller local ISPs. Each ISP is legally obligated to implement its own filtering mechanisms, leading to diverse and sometimes inconsistent outcomes across the network at any given moment. For example, some of Google's services appear to be unavailable to Chinese users nearly always, including Google News, the Google cache (i.e., our service that maintains stored copies of webpages), and Blogspot (the site that hosts weblogs of Blogger customers). Other services, such as Google Image Search, can be reached about half the time. Still others, such as Google.com, Froogle, and Google Maps, are unavailable only around 10% of the time.

Even when Google is reachable, the data indicates that we are almost always slower than our local competitors. Third-party measurements of latency (meaning the delay that a user experiences when trying to download a webpage page) suggest that the average total time to download a Google webpage is more than seven times slower than for Baidu, the leading Chinese search engine.

Users trying to get to Google will have different experiences at different times of day, and from different points on the Chinese network. For example, access to Google appears to be speedier and more reliable in Beijing than in Shanghai, and generally better in the largest cities compared to smaller towns, suburbs, and villages.

---

[8] Id. at 100.

Based on our analysis of the available data, we believe that the filtering performed by the international gateway ISPs is far more disruptive to our services than that performed by smaller local ISPs. Because Google's servers have, to date, been located exclusively outside China, all traffic to and from Google must traverse at least one of China's international gateway ISPs. Accordingly, Google's access problems can only be solved by creating a local presence inside China.

Operating without a local presence, Google's slowness and unreliability appears to have been a major – perhaps the major – factor behind our steadily declining market share. According to third-party estimates, Baidu has gone from 2.5% of the search market in 2003 to 46% in 2005, while Google has dropped to below 30% (and falling).[9] The statistics are even more dire among the college-age young, who use Baidu even more, and Google less, than their elders. Part of this has been due to improvements in Baidu's services and a major marketing campaign (funded by the proceeds of its successful IPO in the US), but the leading cause seems to be the Chinese users' annoyance at the persistent slowness and unreliability of Google.

Google's Calibrated Approach

In light of the chronic access problems that have plagued Google in China, Google's management set out more than a year ago to study and learn about China, to understand and assess our options, to debate their relative merits, and to make a decision that properly weighs both business and ethical considerations.

There is no question that, as a matter of business, we want to be active in China. It is a huge, rapidly growing, and enormously important market, and our key competitors are already there. It would be disingenuous to say that we don't care about that because, of course, we do. We are a business with stockholders, and we want to prosper and grow in a highly competitive world.

At the same time, acting ethically is a core value for our company, and an integral part of our business culture.

Our slowness and unreliability has meant that Google is failing in its mission to make the world's information accessible and useful to Chinese Internet users. Only a local presence would allow Google to resolve most, if not all, of the latency and access issues. But to have a local presence in China would require Google to get an Internet Content Provider license, triggering a set of regulatory requirements to filter and remove links to content that is considered illegal in China.

So we were confronted with two basic options – [1] stay out of China, or [2] establish a local presence in China – either of which would entail some degree of inconsistency with our corporate mission. In assessing these options, we looked at three fundamental Google commitments:

---

[9] CNNIC Search Engine Study.

(a) Satisfy the ***interests of users***,
(b) ***Expand access*** to information, and
(c) Be responsive to ***local conditions***.

The strongest argument for staying out of China is simply that Google should not cross the line of self-censorship, and should not be actively complicit in imposing any limits on access to information. To be clear, the persistence of severe access problems amid fierce competition from local alternatives suggests that the consequence of this approach would be the steady shrinking of Google's market share ever closer to zero. Without meaningful access to Google, Chinese users would rely exclusively on Internet search engines that may lack Google's fundamental commitment to maximizing access to information – and, of course, miss out on the many features, capabilities, and tools that only Google provides.

On the other hand, we believe that even within the local legal and regulatory constraints that exist in China, a speedy, reliable Google.cn service will increase overall access to information for Chinese Internet users. We noted, for example, that the vast majority of Internet searches in China are for local Chinese content, such as local news, local businesses, weather, games and entertainment, travel information, blogs, and so forth. Even for political discussions, Chinese users are much more interested in local Chinese Internet sites and sources than from abroad. Indeed, for Google web search, we estimate that fewer than 2% of all search queries in China would result in pages from which search results would be unavailable due to filtering.

Crucial to this analysis is the fact that our new Google.cn website is an **additional** service, **not a replacement** for Google.com in China. The Chinese-language Google.com will remain open, unfiltered and available to all Internet users worldwide.

At the same time, the speed and technical excellence of Google.cn means that more information will be more easily searchable than ever before. Even with content restrictions, a fast and reliable Google.cn is more likely to expand Chinese users' access to information.

We also took steps that went beyond a simple mathematical calculus about expanding access to information. First, we recognize that users are also interested in transparency and honesty when information has been withheld. Second, users are concerned about the privacy, security, and confidentiality of their personal information. Finally, users want to have competition and choices, so that the market players have a strong incentive to improve their offerings over time.

Transparency. Users have an interest in knowing when potentially relevant information has been removed from their search results. Google's experience dealing with content restrictions in other countries provided some crucial insight as to how we might operate Google.cn in a way that would give modest but unprecedented disclosure to Chinese Internet users.

Google has developed a consistent global policy and technical mechanism for handling content deemed illegal by a host government. Several of the countries in which we operate have laws that regulate content.

In all of these countries, Google responds similarly. First, when we get a court order or legal notice in a foreign country where we operate, we remove the illegal content only from the relevant national version of the Google search engine (such as Google.fr for France). Second, we provide a clear notice to users on every search results page from which one or more links has been removed. The disclosure allows users to hold their legal systems accountable.

This response allows Google to be respectful of local content restrictions while providing meaningful disclosure to users and strictly limiting the impact to the relevant Google website for that country. For China, this model provided some useful guidance for how we could handle content restrictions on Google.cn in way that would afford some disclosure when links have been removed.

Privacy and Security. Google is committed to protecting consumer privacy and confidentiality. Prior to the launch of Google.cn, Google conducted intensive reviews of each of our services to assess the implications of offering it directly in China. We are always conscious of the fact that data may be subject to the jurisdiction of the country where it is physically stored. With that in mind, we concluded that, at least initially, only a handful of search engine services would be hosted in China.

We will not store data somewhere unless we are confident that we can meet our expectations for the privacy and security of users' sensitive information. As a practical matter, meeting this user interest means that we have no plans to host Gmail, Blogger, and a range of other such services in China.

Competition and Choice. Internet users in China, like people everywhere, want competition and choices in the marketplace. Without competition, companies have little incentive to improve their services, advance the state of the art, or take innovative risks. If Google were to stay out of China, it would remove powerful pressure on the local players in the search engine market to create ever-more-powerful tools for accessing and organizing information. Google's withdrawal from China would cede the terrain to the local Internet portals that may not have the same commitment, or feel the competitive pressure, to innovate in the interests of their users.

The Decision: What Google Is Doing in China

The deliberative process and analysis outlined above led to the following decisions.

(1) ***Launch Google.cn.***

We have recently launched Google.cn, a version of Google's search engine that we will filter in response to Chinese laws and regulations on illegal content. This website will supplement, and not replace, the existing, unfiltered Chinese-language interface on

Google.com. That website will remain open and unfiltered for Chinese-speaking users worldwide.

(2) ***Disclosure of Filtering***

Google.cn presents to users a clear notification whenever links have been removed from our search results in response to local laws and regulations in China. We view this a step toward greater transparency that no other company has done before.

(3) ***Limit Services***

Google.cn today includes basic Google search services, together with a local business information and map service. Other products – such as Gmail and Blogger, our blog service – that involve personal and confidential information will be introduced only when we are comfortable that we can provide them in a way that protects the privacy and security of users' information.

Next Steps: Voluntary Industry Action

Google supports the idea of Internet industry action to define common principles to guide the practices of technology firms in countries that restrict access to information. Together with colleagues at other leading Internet companies, we are actively exploring the potential for guidelines that would apply for all countries in which Internet content is subjected to governmental restrictions. Such guidelines might encompass, for example, disclosure to users, protections for user data, and periodic reporting about governmental restrictions and the measures taken in response to them.

Next Steps: U.S. Government Action

The United States government has a role to play in contributing to the global expansion of free expression. For example, the U.S. Departments of State and Commerce and the office of the U.S. Trade Representative should continue to make censorship a central element of our bilateral and multilateral agendas.

Moreover, the U.S. government should seek to bolster the global reach and impact of our Internet information industry by placing obstacles to its growth at the top of our trade agenda. At the risk of oversimplification, the U.S. should treat censorship as a barrier to trade, and raise that issue in appropriate fora.

Mr. SMITH OF NEW JERSEY. Thank you very much.
Now, Mr. Chandler?

TESTIMONY OF MR. MARK CHANDLER, VICE PRESIDENT AND GENERAL COUNSEL, CISCO SYSTEMS, INC.

Mr. CHANDLER. Chairman Smith, Chairman Leach, Ranking Members Payne and Faleomavaega, my name is Mark Chandler, and I am Senior Vice President and General Counsel of Cisco Systems. We have also submitted a statement for the record, and I will, therefore, offer a brief summary of views this afternoon.

We appreciate the opportunity to address these very serious issues. Cisco strongly supports freedom of expression on the Internet, and we respect the conviction of those who have brought these concerns forward.

The Committee is exploring the question of Chinese Government censorship of the Internet. In that regard, Cisco does not customize or develop any specialized or unique capabilities in order to enable different regimes to block access to information. Cisco sells the same equipment to China that we sell worldwide. Cisco is not a service or content provider or network manager, and Cisco has no access to information about individual users of the Internet.

Cisco does aspire to provide open access to the world's information resources to all people everywhere. We support the UN Global Compact on Human Rights, and we comply fully with all of our national laws, which, in the interest of both national security and human rights, prohibit the sale of our products to certain destinations and users, and that includes the Foreign Relations Authorization Act passed by the Congress in the wake of the Tiananmen Square incident.

Cisco was founded 22 years ago by two computer scientists at Stanford in order to enable communication between different computer systems. Today, we have 40,000 employees, nearly 30,000 of whom are here in the United States, and annual sales of almost $27 billion, and our mission of connecting the world has not changed.

Some describe us as the plumbers of the Internet since our technology constitutes the pipes that connect Point A to Point B. Our products were first used in private corporate networks, but when the public Internet emerged in the nineties, our products found worldwide application. When you send an e-mail in your office to your children or grandchildren, that e-mail is routed through equipment provided by Cisco or our competitors.

Because our products are designed to interconnect and expand communications systems worldwide, we build to open global standards. Almost a billion people use the Internet today. The key to the Internet's success today, and to expanding free expression in the future, is standardization on one global Internet, including China, and that remains the core of Cisco's mission.

Now, networks cannot function without network management and security protection capabilities. Otherwise, network administrators could not protect us against hackers who want to try to shut down the Internet or steal personal information. Companies could not stop employees from illegally downloading music of video that is copyrighted or from accessing computer viruses. Libraries

and parents could not control access to pornography. This generic blocking capability is available from all major manufacturers, including at least a dozen United States, Canadian, European, and Chinese companies.

These same capabilities which are essential to operate a network are used in some countries to censor political expression on the Internet. While this hearing is focused on China, the issue is, unfortunately, global. As you have heard, some Middle Eastern countries block sites which are critical of their leadership, for example. Cisco, however, has not, and does not, design products for the purpose of political censorship.

Because of threats to networks around the world, there is no safe way to disable those capabilities that may also be used to block access for political reasons. While I cannot speak to the many other companies who have been cited as providing these sorts of functions to the Chinese authorities, these capabilities in Cisco's equipment are off the shelf, and their designated uses are essential.

I will close with one observation. Legislation or other action which encourages governments to build their own Internets will reduce free expression. Last year, the Chinese authorities proposed a special standard to allow Chinese companies alone to manufacture certain equipment for accessing the Internet. Our Government resisted that proposal, and we urged continued action in that regard. The power of the Internet to expand free expression depends on there being one global Internet.

Efforts are underway, often driven by anti-U.S. activists, to balkanize the Internet. Policies which promote that, even inadvertently, will undermine rather than support the many projects which you cited, Chairman Smith, and which Congressman Rohrabacher cited which help users evade censorship.

Around the world, those who fear the liberating power of ideas will seek to use their own power to block free expression. With the right policies, censorship will fail. The Internet is not just a source of information, but it is a beacon of hope, and we must do everything we can to keep it that way. Thank you.

[The prepared statement of Mr. Chandler follows:]

PREPARED STATEMENT OF MR. MARK CHANDLER, VICE PRESIDENT AND GENERAL COUNSEL, CISCO SYSTEMS, INC.

Mr. Chairman, Members of the Subcommittee:

My name is Mark Chandler, Senior Vice President and General Counsel of Cisco Systems. Thank you for the opportunity to address some very important and difficult issues. Cisco strongly supports free expression and open communication on the Internet, and we respect the strength of conviction of those who have brought these concerns forward.

The Committee is exploring the question of Chinese government censorship of the Internet. In this regard:

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

Cisco *does*, however, comply with all U.S. Government regulations which prohibit the sale of our products to certain destinations, or to certain users or to those who resell to prohibited users. We have not sold and do not sell our equipment to the countries listed on the U.S. Department of Treasury's OFAC (Office of Foreign As-

sets 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 the Tiananmen Square incident.

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. We do not design custom or closed Internet systems. The Internet technology may not be perfect—and the Internet itself can be misused—but there has been no greater force in spreading the power of ideas than the single worldwide Internet. The key to its growth and the flow of information it enables has been the standardization of one global network. This has been and remains the core of Cisco's mission.

Cisco was founded 22 years ago by two computer scientists at Stanford University who were seeking a way to exchange information between different computer systems in two different departments. At that time, such communication was very difficult if not impossible even within a college campus, although today it is, of course, common across the world. Our founders developed a device to communicate between their disparate computer systems. This became the first product of Cisco Systems, known as a router. Today we are a leading supplier of Internet equipment. We employ nearly 30,000 people in the United States and 10,000 overseas. We have annual sales of approximately $27 billion, and we hold over 2,000 issued US patents and have applied for over 3,000 more.

Networking equipment (routers and switches) forms the core of the global Internet and most corporate and government networks. Cisco makes the equipment that makes the Internet and networking work. We are often described as the "plumbers" of the Internet, as our technology constitutes the "pipes" that connect point A to point B. Originally our products were designed for communications within private or enterprise networks. When the public Internet emerged in the mid '90s, our products found immediate application for worldwide use. We now have many competitors around the world who build products that perform similar functions. When you send an email in your office to your children or grandchildren, the digital language that makes up that email is routed through equipment made by Cisco or our competitors.

Networks that existed in the early 1970s would eventually evolve into the Internet, but at the time Cisco was founded, the Internet as we know it today did not exist. As the Internet grew, it moved from societal novelty to a critical part of the communications infrastructure of our country and the world. It unfortunately also became the target of attacks, the intended result of which was to attempt to reduce its capability to operate by impeding or entirely preventing its ability to provide communications services to millions of users. These attacks can take many forms, some of which are referred to as worms, viruses, denial of service attacks, and more. Network management and security capabilities—including technology generically referred to as filtering—are essential to mitigate attacks and thus enable information flow. No network can be administered without the ability to manage and protect the information that flows through it. Without this capability, it would not be possible to operate the Internet and the Internet would likely not exist as it does today.

The technology that is used to manage and protect against hackers or websites that host viruses is also the same generic technology that allows libraries and parents to filter or control internet access by children, such as via AOL's parental controls, or block pornography or the illegal downloading of copyrighted material. If, for example, a network administrator knows that a certain website is dangerous to her network because a virus or spyware has been downloaded from that site, or because the site is pornographic, she can use IP address blocking (each website and user on the Internet has an IP—Internet Protocol—address—the equivalent of a phone number) to protect her network from that site. This technology is a customary part of network management software of all major suppliers of Internet equipment—Cisco's and our competitors'—and is basic to network functionality. Whether for security or the management of information, the technology is one and the same. The filtering that occurs is implemented by the owner or administrator of the network using technology that is available regardless of the manufacturer.

Some countries have chosen to restrict or limit access to information on the Internet based on political considerations, rather than on the freedoms that we enjoy in this country. While many have commented on the activities of the Chinese government in this regard, the issue is, in fact, global. Some Middle Eastern countries block sites critical of their leadership. And judicial action has been taken in France due to the failure of an operator to block French users' access to some types of information. Cisco however has not and does not design products to accommodate political censorship. The tools built into our products that enable site filtering are the

same the world over, whether sold to governments, companies or network operators. The features in our equipment are "off the shelf" and not altered in any way for any market or region. Similar technology is available from at least a dozen other US, Canadian, European and Chinese companies. Because of threats to network operations, which exist around the world, there is no way to market equipment without these capabilities. The management of information flow by a customer cannot be prevented by Cisco unless we are to also prevent the originally intended use of this technology, which would expose the Internet to the full risks of inevitable daily attacks. Networks attached to the Internet would literally stop working.

Our innovative products have helped lead the world into the Internet age and are truly changing the way the world lives, works, learns and plays. For instance, since our entry into the Chinese market in 1994, the number of Chinese accessing the global Internet has grown from 80,000 in 1995 to over 130,000,000 in 2005—a 1625% increase in the past 10 years. While Cisco certainly cannot take credit for all of the Internet growth in China, it shows that the appetite for information via the Internet is nearly impossible to contain. Is there any question that the Internet has provided to hundreds of millions of people access to information from around the world in a volume and with a speed unthinkable even a decade ago?

For some, the Internet is a tool that liberates individuals from the constraints of time and distance, empowering those who previously had no access to the world's store of information. Some are fearful of this liberation as they see the Internet as a mechanism for empowering non-state actors. Still others see the Internet as a tool used by governments to control content.

Any policy response to this divergence in views is necessarily complex. It must, however ensure the continuation of a single, worldwide Internet if the goal of global free expression is ever to be achieved. Among the questions most pertinent: Has the Internet helped spread a dramatic increase in access to information in regions where content is nonetheless subject to certain limitations? Does active engagement in such countries help to influence policy decisions? What policies will best help foster the ability to overcome censorship? If countries that engage in censorship are to be denied US Internet technology, will those countries establish closed-standard Internets of their own to further restrict access to information? In our view, legislation or other action which encourages governments to build their own Internets will reduce free expression. Last year, the Chinese authorities proposed a special standard to allow Chinese companies alone to manufacture Internet equipment for China involving the use of encryption. Our government resisted that proposal, and we urge continued action in that regard. The power of the Internet to expand free expression depends on there being one global Internet. Efforts are underway, as illustrated in the attached article, to balkanize the Internet. Policies which promote that—even inadvertently—will undermine rather than support the many projects which help users evade censorship and will exacerbate rather than solve the problems we are discussing today.

The liberating power of the Internet depends on its existence as one global Internet. Its advent is a powerful force and its capabilities broad. Any policies in this area should, we believe, proceed from the realization that its very global nature provides a unique tool for the dissemination of ideas and cultivation of freedoms. We should do nothing to disturb its promise.

Thank you for inviting us to appear before you today.

Mr. SMITH OF NEW JERSEY. Thank you very much for your testimony. Thank you all for your testimony.

First of all, before I ask some questions, if we could just dim the lights for a moment, I just want, for the purposes of the Members who have not done this—I spent several hours doing it myself 2 days ago and last week—if you go to google.cn and also go to google.com and ask the same or put in the same phrase or word, you get two entirely different outcomes.

If you put in "Tiananmen Square" and go to google.com, which is obviously what is available to every one of us here, you get pictures of the atrocities that were committed in Tiananmen Square against peaceful protestors. Let me just say parenthetically, I mentioned at the outset that I have held a number of hearings on human rights issues in China.

One of those hearings was when Choha Tien, who was the defense minister of the People's Republic of China, came and visited, he got a 19-gun salute by the Clinton Administration, which I thought was inappropriate. But he said at the Army War College that nobody died in Tiananmen Square. Well, at home, he is used to getting away with that kind of information and those kinds of big lies, but immediately he was challenged by many of us.

I convened a hearing 2 days later right here in this room. We had several people who were on the square that day, including journalists and activists, including one who is in the room right here today, and *Time Magazine* correspondents, and we asked Choha Tien or anybody from the Chinese Embassy to come and give an accounting for such a big lie. Nobody showed up from the Chinese Embassy. Choha Tien did not show up.

But it underscored to me that at home they are used to getting away with it; abroad, they need to be challenged because, obviously, many of us who followed those occurrences knew that there was a different set of circumstances, and the truth was entirely different from what was represented.

You go to google.cn, and you get pictures of people in Tiananmen Square smiling, wonderful pictures of the square, but you do not get pictures of what really happened that day.

Mr. Schrage said a moment ago there is a handful of politically sensitive requests. Well, they are, in many ways, all important. It has to do with the Falun Gong, China human rights issues, the use of torture, which I said to the previous panel, under Manfred Nowak, and he is just the most recent person to report on it, the UN Special Rapporteur on Torture, and he says it is widespread.

I would recommend to my friends who are at the witness table here to read the State Department's Annual Report on Human Rights Practices as well as the Religious Freedom Report and the Report on Trafficking. It paints a horrific picture of systematic human rights abuses in China, which the question is, are we enabling, or are we providing some kind of counter to it so that the flower of a generation, those students and young men and women who aspire to nothing more than human rights, are not put into prison but, instead, are lifted up and hopefully get an airing of their concerns.

So let me just go to some questions, and if you gentlemen would not mind responding to those questions, and time being what it is, I will lay out my first major question and then the second and then yield to you and then go to my good friend, Mr. Payne.

Harry Wu, who is the great survivor of the Laogai, spent 19 years in the Laogai and, again, in the 1990s, was able to assemble six survivors of the Laogai right where you sit. Paul D'Angiotso and I chaired that hearing. Paul D'Angiotso was a Buddhist monk who could not even get through the security downstairs because he brought the implements of torture that are routinely employed against both women and men: Cattle prods applied to the genitals, under the arms, and in various other sensitive places. He brought those and said, "This is what is used day in and day out against people in the Laogai." Remember, there are at least 6 million, some say many more than that, in the Laogai today, including political and religious dissidents, including Shi Tao.

Harry Wu will testify later on today, and I quote him:

> "A friend of mine recently tried to access some 'politically sensitive Web sites' while at an Internet cafe in a remote, small city in Xinjiang Province. The police quickly showed up to arrest him. I do not know who supplied the technology enabling the police to track my friend's Internet surfing, but I am pretty sure that U.S. technology was involved."

He goes on to point out that Golden Shield, which monitors Chinese civilians, had assistance from Intel, Yahoo!, Nortel, Cisco Systems, Motorola, and Sun Microsystems, and he says, "The Golden Shield project would not have been possible without the technology and equipment from these companies."

So my questions are, exactly how does the secret police track Internet users, e-mail searchers' sites, and does your technology of your respective companies and presence in China in any way enable or assist the Chinese police in this endeavor?

Secondly, and this might be more to Yahoo!, but the others might want to provide an answer as well, how does the secret police monitor Yahoo! e-mails? Do they have access to your files, your cyber files and to private information? How many times do they—"they" being the police—request information that is in your files? Is it routine? Is it every day? Do they have some automated way of just doing it without even making a request? Do you ever say no? Are there circumstances around which you would say, "No," and say, "We are not going to provide the information. This is a political prisoner or a political personage. We think that the nature of this request crosses a line. We do not just say yes to everything."?

Are any of the names among the known cyber dissidents and journalists? Reporters Without Borders suggests that 39 cyber dissidents, and I forget the number of journalists, but large numbers, but as I said, and I will say it for the third time, many of us believe that is the tip of the iceberg. Have you ever tried to cross-reference any of those who are now in the Laogai or in a jail somewhere else with those requests that were made to any of your respective companies?

With regard to Google and Internet filtering, who decides and how often and where what is now going to be blocked. What bureau within the People's Republic of China does the blocking? For instance, Tiananmen. Who were the ones who said, Tiananmen, that is a no-no? You cannot have that. And how many words are we talking about, and can that be expanded from day to day? For example, if the police raid a small village, as they have done recently, and kill people, all of a sudden the People's Daily does not over that, and that is to whom many of your Internet users in China will be sent or China.com. Who makes those decisions? Is it you? Is it the people in China, the government?

Why do you send Internet users, and I ask this very respectfully, why do you send them to government propaganda sites, when I or anybody in this room go to google.cn, go to the disinformation site? Many of us are concerned about torture. Manfred Nowak—again, I will use his name—UN Special Rapporteur on Torture. A scathing report on China just came out in December. If you put his name in google.cn, you go to a People's Daily report about he wants

to go to Guantanamo, and I think and many others in this room certainly think he ought to be able to go to Guantanamo. I have gone there. Many Members of Congress and many journalists have gone there. He ought to be allowed to go there.

But the big question is, why is it that you get sent to that site, which completes the loop? And with so many young people using the Internet, they are now getting the party line, and that party line usually puts the United States in a very, very bad light.

Finally, are you gentlemen aware of just how widespread torture really is in China? If you or I were arrested, what I am saying right now would fetch me a 15-year term in the Laogai, no questions asked, maybe longer, as well as what others, especially on our third panel, the human rights activists. If Harry Wu goes back after speaking today, he will be nabbed and sent right to the Laogai and will be tortured. That is the day-to-day practice.

I deeply respect that your companies do so much good and provide freedom of information in so many ways. I have a Yahoo! e-mail account, also an MSN e-mail account, as does my wife, but in a repressive country we are talking about a situation where it becomes a tool of that repressive regime. As I said at the outset, and I think it bears repeating, propaganda and secret police are the two main pillars of any dictatorship anywhere in the world, and that includes the PRC.

So if you could go down the line and answer some of those questions.

Mr. CALLAHAN. Congressman, first off, Mr. Chairman, I will answer the questions with respect to Shi Tao, in particular. You directed those at me.

Let me please state in no uncertain terms, as I did in my testimony, that our company condemns the persecution of any person for exercising their right of free expression, whether in China or anywhere else in the world. You asked about how this information is disclosed. Against the backdrop of the fact that I no longer have supervision over the day-to-day operations in Beijing following our transaction in October, but when we did have control over the day-to-day operations, we made sure that our Beijing operation would only comply with a lawful demand from an authorized agency. The demand had to be in writing, the demand had to have a seal of the agency, and the demand had to come from someone we had made sure was an authorized representative.

There was no ongoing access to the Yahoo! files by Chinese law enforcement. These were requests, demands that we had to comply with, and no one is more troubled by this, Mr. Chairman, than when we realized this came out in the news that we had supplied information pursuant to a lawful demand that had been used for this purpose.

When we established operations in Beijing, we made sure that we had this process in place. I can assure you that was unpopular with the Chinese Government, with the law enforcement authorities we dealt with. It was not the practice of the other companies, local companies, in the market at that time. We did take some heat for that. I would not be remiss to say that.

Furthermore, we have no knowledge of the identity or the purpose of the investigation when they came to demand this informa-

tion about Mr. Shi Tao, in particular. In addition, we followed the rigorous procedural process that we had in place, and as a backdrop, I do not think it would be appropriate for me to sit in my office in California and order a Chinese citizen in our Beijing operations not to follow a lawful demand, recognizing the very distressing consequences that that caused, that could subject that person to persecution and criminal prosecution. And for that reason, Mr. Chairman, we wanted to take this issue, address it head on.

By no means do we come here today and say that these are good consequences. These are horrible and distressing, but by the same token, it exemplifies for us why Yahoo! cannot take this issue on by itself, Mr. Chairman. We ask for the government's help. We are encouraged by the State Department's announcement, and we are here and ready to engage with our industry peers on this topic.

Mr. SMITH OF NEW JERSEY. Before moving on, just very briefly, it is my understanding that Google has made a different determination because they have not sited their e-mail servers inside of the repressive country, in this case, China, so that access to what you term a legitimate request from law enforcement. Part of the problem we have is that law enforcement is enforcing unjust rules and regulations and laws, and there is a difference. To enforce apartheid 20 years ago or more on South Africa was profoundly unjust, and yet it was a rule of law. So if it is an unjust law, somehow we would suggest, and one of the things our bill would do would be to put e-mail servers out of harm's reach to the greatest extent possible.

In terms of Alibaba, you mentioned in your testimony, and then I will move down the line, not to belabor it, that you talked to them. What is their response? You did not say what that was. In a way, does that give you some plausible deniability because you are still a shareholder in Alibaba? Again, I mentioned IBM and the Holocaust. One of their plausible denials was that they had IBM Germany that was doing much of the heavy lifting when it came to creating a data base which included Jews that regrettably were marched off with incredible precision, and the trains did run on time to the gas chambers.

Mr. CALLAHAN. Mr. Chairman, as I mentioned in my testimony, I met with senior executives at Alibaba, as did other senior executives at Yahoo!, to express our concern about these issues and to encourage them to follow the very rigorous procedural protections that we had in place when we controlled the operation. I cannot speak for them. I hope that they will follow that. I think they recognize how important it is to Yahoo! as a major shareholder, and I believe that has some influence on that.

As to the second part of your question, Mr. Chairman, about the transaction itself, plausible deniability is not a factor for Yahoo!. I come to this Committee today to recognize the distressing consequences of having to comply with this law enforcement demand. We recognize that we need to do our part as part of the industry in working with government to address the situation. That is how we come to you.

Mr. SMITH OF NEW JERSEY. Would it be correct to assume you do not know how many times the police make requests and how often those requests have been honored and whether or not any of

that marries up with people who we know to be imprisoned as a result of e-mails that were captured by the secret police?

Mr. CALLAHAN. That is correct. Because we do not receive the identity or the reason for the investigation, as well as the fact that the records are not in our control, it is not information——

Mr. SMITH OF NEW JERSEY. Do you keep a record at least of how many investigations there have been?

Mr. CALLAHAN. The records are kept at the local subsidiary, so it is——

Mr. SMITH OF NEW JERSEY. Could we get that for the Committee?

Mr. CALLAHAN. It is my understanding, sir, that those records are prohibited from being disclosed under Chinese law because they are demands from Chinese law enforcement.

Mr. SMITH OF NEW JERSEY. So we will not even know the scope and the magnitude of how many requests have been made and how many times pertinent information has been tendered to the Chinese secret police. Is that, in and of itself, not enough to move out and disengage?

Mr. CALLAHAN. Congressman, we believe firmly that the benefits that the Web brings are very, very important, and we believe that having a presence in countries, and it is not just about China, and it is part of the reason we set out principles and commitments that we wished to make, that engagement is the better course. We recognize these very serious consequences, but we are also here to recognize that we share responsibility to engage with government on this issue.

Mr. SMITH OF NEW JERSEY. Finally, do you know how the Chinese Government knows which e-mails to make requests on?

Mr. CALLAHAN. I do not have that information.

Mr. SMITH OF NEW JERSEY. Could you provide that for the record?

Mr. CALLAHAN. It is not information that we would have. We received a lawful request for a certain user ID.

Mr. SMITH OF NEW JERSEY. But how are they monitoring? That is my question.

Mr. CALLAHAN. I do not know the answer to that question.

Mr. SMITH OF NEW JERSEY. If anybody else knows, I do hope you will provide that for us. Thank you.

Mr. KRUMHOLTZ. Mr. Chairman, let me, in response to your question, perhaps take you through how we respond to requests from Chinese authorities.

When we receive a take-down directive in China, we generally only have 24 hours, sometimes less, to respond. We review these requests at our Chinese operations center and also at Microsoft headquarters to assure that the appropriate authorities are involved and that we have no basis to challenge that conclusion.

I should note that most blog take-downs are actually things that we do when there has been a violation of our terms of use, when a blogger has content that raises questions of racism or bigotry or pornography. So the overwhelming majority of our take-downs involve a violation of our own terms of use.

Customers' personal information is stored on servers located in the United States, so requests for that information from the Chi-

nese have to be handled under procedures that are provided under the U.S.-China Mutual Legal Assistance Treaty. Since we are the U.S. Government, the U.S. Department of Justice engages, and we would follow their orders if they determined that we should provide that information.

Finally, in a very limited number of cases, and this is not just in China but wherever we do business, and we do business in over 90 countries, we do cooperate with local law enforcement agencies when an individual's personal safety is at risk. So, over the past 2 years in China, I believe there have been about a half a dozen cases—there has been a case of murder, a missing American student, or pornography or other serious crimes, crimes of a serious nature, where we will cooperate with the local law enforcement agents.

Mr. SMITH OF NEW JERSEY. Does Microsoft provide any capability to monitor e-mails or any other information that is flowing through the 'Net in China?

Mr. KRUMHOLTZ. We do not.

Mr. SMITH OF NEW JERSEY. Thank you. Mr. Schrage?

Mr. SCHRAGE. So, candidly, we are new to the market, being on the inside, and we have developed our program in a very calibrated way to be consistent with the values and the missions I described earlier on. As a practical matter, we have agreed to enter the market to perform search services, but we made a fundamental, strategic decision that we were not going to offer services like G-mail or Blogger, services that provide us commercial value, benefits in other arguments, that we would not provide those services inside of China because we did not want to be put in a position where we would have possess of data that might create the kinds of problems we are discussing today. I want to be categorical in that.

That deals with the first set of issues that you have asked about, privacy and confidentiality of information. We are not going to have it, so we are not going to be in a position to give it.

The second set of issues you asked had to do with censorship, and, again, as I mentioned earlier, it is an issue that we have great concern.

I do want to make some reference to your point earlier on about google.com and google.cn. I am actually very proud of what you just showed because, in contrast to every other search engine in the marketplace, we make it very clear and very easy for anyone anywhere in the world to see what is and is not available in China. It is not something we are happy about. I want people to know the kinds of problems that we are forced to deal with in China so that you, and perhaps with my colleagues here in industry, we can seek to make the same information available in both services.

With respect to who decides and what is on the list, it is actually a somewhat straightforward process. What we do is we base our service inside of China, and we begin to search. We try to find the information that is already available to users that passed through the firewall. Internally, there is no firewall—it is already restricted—and externally.

As a practical matter, from that we derive a list of sites, of URLs, that are just blocked by the Chinese firewall, and what we have done is we have essentially, and I am somewhat oversimpli-

fying, we have essentially made available inside of China those things that we have found that are either already available or were not blocked but were otherwise unavailable. Other search engines did not capture that information, either inside of China or outside.

The last point you make, frankly, is, candidly, the most troubling one, and one I do not have a great answer for you. You made an excellent point, Mr. Chairman, earlier on: Is a half truth better than no truth? Is it better to have half the results that are misleading than to have no results at all? That is a very appropriate question to ask and one that I do not have an answer for you today. I think that is precisely the kind of question that would be an appropriate subject for an industry group to discuss, precisely an appropriate question for the State Department task force to discuss, and we would be delighted to be a part of that conversation.

Mr. CHANDLER. Mr. Chairman, your question, as I understood it, was related to the technical means by which filtering is undertaken with respect to Cisco products. Customers around the world use embedded filtering that is part of network managing software to manage their networks, as I alluded to. I understand, for instance, in the House of Representatives that if you or staff seek to reach sites that include spyware that would be loaded onto your computer, it is automatically blocked. That is a good thing, and I think we all understand why that happens.

The programming of it, which is undertaken by users, at least as it relates to our products, is so-called "URL filtering" where particular Internet addresses, if they are known, IP addresses or URLs, universal resource locators, can be programmed in so that those sites cannot be reached by the user trying to reach those sites. That is the principal mechanism available worldwide as part of network management software not just from Cisco but from really every vendor, Chinese, European, American, because it is so fundamental to Internet security.

Mr. SMITH OF NEW JERSEY. If I could ask you, in terms of tracking people as they move along the 'Net, is there any capability that you have provided that allows the Chinese dictatorship, the secret police, to say, so-and-so just asked about the Falun Gong? Now we know what their IP address is, who they are, and the next thing you know, somebody shows up at the door.

Mr. CHANDLER. I think the questions that get asked to some of the service providers are illustrative of the fact that the information is not readily available from the network. There are products which I am told we do not supply to service providers in China which are available for so-called "content searching." There are a number of them from a number of different companies. Enterprises use them to manage their internal networks. We do not provide it to service providers, but that will allow for content searching within particular documents that are passing through a network.

Mr. SMITH OF NEW JERSEY. Let me just ask in terms of Police Net, what kind of capabilities does that give to the public security police, which we know brutalize people, especially religious believers, especially groups like the Falun Gong? Hundreds of Falun Gong have been tortured to death, not only to crippling and people who walk around with post-traumatic stress disorder, but to death. They have done it with many, many others as well of different reli-

gious faiths. Sitting where you are sitting, besides people like Harry Wu, we have had Wei Jingsheng and others testify before who talk about the brutality that happens every day.

I went on Google and downloaded where I was sent when I put in "human rights" and came to this judicial reform and interest of human rights, and it has smiling policemen on page after page almost holding town meetings, which is a Potemkin Village in and of itself about what these police are really all about. Officer Friendly; it just does not comport with reality.

My question is with regard to the tracking, if any of you could get into that further, if you would, of these individuals and Police Net, in particular. We are told, and please correct me if I am wrong, this has linked all of the public security police in a way that they had not heretofore, which gives them, again, an efficacy and an ability to track real criminals but also the other edge of the sword, human rights activists so that they silence dissent.

Mr. CHANDLER. The phrase "Police Net" is not a Cisco expression. I can explain what types of products we sell to law enforcement around the world and how those might have application. We sell data networking products. We are a networking company, and we try to illustrate for our customers ways that data networking can be used to improve operations.

With respect to law enforcement and first responders, generally our focus has been on providing products that allow data networking to permit greater access to information resources. So, for instance, a product will allow an ambulance driver to be able to see medical records of a patient, will allow police to be able to access resources that are in law enforcement data bases officially, and our products bring together voice-video so, for instance, if there is a closed-circuit television system or a Web equivalent of that, those images can be seen by a mobile law enforcement agent. But it is data networking. We are not a company that provides the data itself or builds data bases, but we provide a networking solution worldwide that allows for data bases to be brought together, both in a fixed and mobile setting.

Mr. SMITH OF NEW JERSEY. Tell me if you think this is accurate. In defensetech.org, they have a statement that says: "Police Net connects officials of the Public Security Bureau, a national agency with local branches that handles security, immigration, social order, and law enforcement . . ."—"social order" is obviously one of those elastic terms—". . . to keep a wealth of information on every citizen in China. Cisco marketed Police Net at China's 2002 Information Infrastructure Expo," and then it goes on from there.

So don't they now have that and are utilizing it?

Mr. CHANDLER. Police Net may be a designation they use inside China for what they are doing. What we sell is a data networking solution that is sold worldwide to law enforcement that includes sales in China, but it is a data networking solution. The data have to exist in order to be networked and brought together and made accessible.

I will say that the Congress, after the Tiananmen Square incident, passed the Foreign Relations Authorization Act that established very, very specific criteria for selling equipment that was considered crime control equipment in China, and there is a list of

products associated with that. None of the elements that we sell in China to law enforcement agencies is considered part of the crime control equipment that was controlled under that act.

Mr. SMITH OF NEW JERSEY. But as you know, the Internet was nowhere near where it is today back then, and the capabilities for law enforcement, in this case, an unlawful law enforcement agency, to crack down on dissidents did not exist. So one of the things we are looking at in our legislation is to expand that list.

Let me ask one other question, and then I will yield to my colleagues, and I appreciate their patience. They will have ample time to ask questions as well.

Both in Google's testimony on page 4, Microsoft's on page 5, and Yahoo!'s made mention of it as well, pointed to the Academy of Social Sciences of China. Google, your testimony: "A recent, well-respected study by researchers at the Chinese Academy of Sciences found that 54 percent of users believe the Internet provides more opportunity to criticize the government." Microsoft: "One recent independent survey of Chinese Internet users, 60 percent of users believe the Internet will provide more opportunities to criticize the government."

Frankly, in going online and looking at greater depth myself at the Chinese Academy of Social Sciences, it turns out that the head of it is a member of the Central Committee. He is a Communist in good standing, if you will, and they also, in their mission statement, talk about how dedicated they are to Marxist-Leninist ideology and the teachings of Mao Tse Tung, and my real question is, do you really believe that a study can be had in China where people are fearful when asked questions like this?

This is not a Gallup poll. How was that study done? You are quoting it with great respect and admiration. Who did they really poll in those five cities that they claim to have polled? We know that answer the wrong way or criticize the government, and you end up in the gulag. So why would they think that at a time when the "'Net is drawing ever closer," and this dragnet is capturing more and more people, that the Internet is going to provide this enhanced ability to do that?

Mr. Krumholtz, in your testimony, you rightfully point out that these all-encompassing, catch-all phrases are used in China. You said "disturbing the solidarity of people." What does that mean? "Harming the interests of the nation." These are the same kinds of catch-all phrases like "slander against the Soviet state" that were employed with impunity by the Soviet Union during their crackdowns on dissidents. So if you could answer that. We have got to be careful who we quote. Do you really have confidence in the validity of that survey?

Mr. KRUMHOLTZ. Mr. Chairman, it is my understanding that this study was founded by the Mark Foundation. It is the fourth year in a row that it has funded a study of this kind. I have a great deal of respect for the work of the Mark Foundation.

That said, the study aside, I think I can point to just our own experience with MSN Spaces. Again, we launched that service in May, and in under 9 months we have over 3.5 million users creating their own individual Web sites, or blogs, and over 15 million unique visitors. The fact of the matter is, at least in our view, that

there is more opportunity for communication and freedom of expression in China today as a result of our service and other services, and we expect the trend just to continue.

Mr. CALLAHAN. Mr. Chairman, I believe my testimony cited that study for a proposition that even the Chinese Government agency had cited that they cannot control the Internet, and that was what we found to be a profound statement by their own research agency.

Mr. SMITH OF NEW JERSEY. Mr. Payne.

Mr. PAYNE. Thank you very much. Therefore, you conclude that even though there is increased jailing of journalists and cyber dissidents, that you think that the number of dissidents and their activity will greatly exceed the government's ability to catch them all and throw them in jail. Is that what you all conclude? We could start on my right and go down.

Mr. CALLAHAN. Our belief, Mr. Congressman, is that the benefits of having access to communication service, as well as access to independent sources of information, coupled with the extreme large number of searches and other activity that happens on the Web, provides an extraordinary benefit.

We recognize these extreme challenges as well, and we are ready to tackle those, along with our industry peers and with government, in partnership to make this a government-to-government dialogue.

Mr. KRUMHOLTZ. I would just reiterate that we think these are very difficult issues, which I think is clear from some of the questions from the Members, but we, too, think, on balance, that it is better for Microsoft and the other companies here at the table and other United States Internet companies to be engaged in China. We think that the benefits far outweigh the downside in terms of promoting freedom of expression.

Mr. SCHRAGE. We made the decision to enter the market because we believe in making information available and accessible. We believe that doing that will achieve positive things. As I said in my testimony and in my oral statement, if, over time, we do not achieve the results that we seek, because your question is a legitimate one, we will reconsider our role there.

Mr. CHANDLER. The Internet is many different things to different people. For some, it is a source of empowerment, enlightenment, giving them access to information they never had before. Others are frightened by that empowerment and see nonstate actors, whether they are multinational corporations or terrorists or antiglobalization activists, empowered against legitimate state authority, and others see the Internet being used as a tool of repression. I think all of those are correct.

Chairman Greenspan referred to the economic, social, and political changes that the Internet has been bringing about as a once or twice a century kind of event, and in making U.S. policy about how best to address all of those different things that the Internet is, a critical element to consider is the effect of those policies on the existence of one global Internet.

We think any regulation that would impair the existence of a global Internet, from an infrastructure standpoint, which is what we provide, and lead to local companies being sole suppliers in their markets for specialized sub-Internets, would basically under-

mine additional free access to the Internet by empowering governments more to come up with their own standards and their own controls and make it harder for the efforts that are out there to evade censorship to succeed. That is the concern I would bring to bear in your consideration of alternative policies.

Mr. PAYNE. Let me ask you, Mr. Chandler, since you were speaking, about Cisco Systems. Although Cisco Systems denied that it has tailored its products to suit the PRC Government's censorship, does your technology in China, in fact, significantly boost PRC's censorship capacities? The reason I raised that question is by building a research and development facility in Shanghai, will Cisco Systems more directly serve the Government of China on the censorship objectives, and if not, why not?

Mr. CHANDLER. The research and development facility in Shanghai will employ about 100 people built up over a 5-year period primarily focused on home networking products and voice-related applications, voice-over-Internet protocol. They are not related to Chinese-specific products for censorship purposes in any way.

From the standpoint of our products and the filtering capability that is embedded in our products, through the customary filtering that network management software allows, we do not see a differentiation between our products in that respect and those of our competitors that is meaningful. Chinese competitors, European, numerous other American companies that have been cited by some of the other people who will speak on the panel following us all provide products that perform very similarly in that respect.

Mr. PAYNE. I am going to yield because our other Chair has to leave, but I just my ask that you do not feel you are more susceptible by being there to have maybe government creep move in, not intentional, but if you are right there, you have got 100 now that decide they want to expand, maybe go to 200. It is set up to be more cozy with the government. I do not see how you can prevent it. Let us put it that way.

Mr. CHANDLER. I understand the concern.

Mr. PAYNE. Mr. Leach, I will yield.

Mr. LEACH. I am not in that great a hurry. Please.

Mr. PAYNE. Okay. I will try to be short. I wonder if Yahoo!, if you had refused to provide the PRC authorities with the personnel information and identification information of Shi Tao, the Chinese journalist we have been talking about that we know is in prison, do you think there would have been ramifications to Yahoo!, and what might they be? And, secondly, would you think that Shi Tao would have been arrested without the specific information that you provided to the government?

Mr. CALLAHAN. Congressman, as to your first question, with respect to—I am sorry. What was the first part of your question?

Mr. PAYNE. That if you had refused to give the information.

Mr. CALLAHAN. I am sorry. It is our understanding that to refuse to comply would have subjected local employees in the local operation to potential criminal prosecution and criminal penalties, including imprisonment.

As to the second question, as to would the prosecution would have happened without the information, I would not be able to speculate as to that.

Mr. PAYNE. Okay. Let me just sort of conclude this general question. Since Yahoo! and Microsoft and Google and Cisco are so important, without you four there, China would be light years behind. We know that perhaps there are laws about restraint of trade or companies coming together because it may be antitrust, but, you know, knowing what the down side is, it would appear that there could have been some creative way that if all four of you said, we are going to withhold this one, or we are not going to roll over on that one, you see, when one goes and opens up, it is just like I work with the Caribbean countries, and this cruise ship business is a big deal. So, you know, Bermuda might say, well, you can dump your garbage here for five dollars a ton, and the others will say, well, I will do it for three, and so they will go to the lowest bidder. You will find that if they all said it is $10 because it is a lot of garbage, and we are going to get what it ought to be, or for every person that comes off the ship we are going to charge you $20. One will say, well, we will do it for 10.

If all of you said, maybe this piece of information, they cannot do it without it, and somehow came with an agreement that, you know, we will all hold hands together and jump off the cliff together. It seems to me that there could have been some way that it could have either slowed down, or our U.S. Government could wake up and try to come to the defense. In other words, it just seems that you have taken the easy way out. A billion, four people. Let us rush over there. Of course, we have got a billion, four in India, too, so I do not know what you are doing there. That is a lot of hits, you know.

None of you are really doing badly, from what I understand. It seems like you all are in kind of good shape; sort of moving forward is the stuff of the future. Has there ever been any kind of an industry discussion? I mean, even cars put air bags in them. People try to protect people, maybe try to have hybrid cars to cut down on fossil fuels, a terrible name for a car, but they are working at trying to be of assistance.

It seems here it is just that we have got to go along to get along. We will just roll over with the government, and that is that. I just do not see the industrial integrity that we should try to find in such outstanding corporations. All of you are competent people, all top folk. Each of your companies have high-level, very professional, competent people. Why just roll over and let the torturers torture? You do not do cattle prods, so you cannot be held responsible because they use them. I mean, what is it?

Mr. KRUMHOLTZ. Congressman, if I may, the companies in our industry have initiated a dialogue to talk about whether or not there are some guiding principles that we can operate under in countries like China. That said, I think we need to take care not to overestimate even a group of companies' leverage with a foreign government, a foreign sovereign. That is why I think all of the companies applauded yesterday's announcement of the Global Internet Task Force by the Secretary of State because we really do think that, working together, the industry, government, and the NGO community could make some real progress here.

Mr. SCHRAGE. Congressman, we are fierce competitors with these guys. We do not usually go bowling together, and so, first, that is a real hurdle that we have to overcome.

Second, as powerful and as important as you think are three companies are, or as we think our three companies are, in China we are not the dominant player in that market. There is another company that is not here today that has a majority of the market share, at least in the search business, so that, frankly, I think that that competitor, that local competitor, would like nothing more than their three American counterparts to go to the Chinese Government and say, we will not cooperate with these restrictions, because that competitor will go to the Chinese Government, I believe, and say, that is great because we will.

That is why we need your help in helping us work together but also supplementing what we are doing.

Mr. PAYNE. Thank you, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. Chairman Leach?

Mr. LEACH. Thank you, Mr. Chairman.

One of the distinctions that has been drawn here is between Mr. Krumholtz and Mr. Callahan, and you have suggested, Mr. Callahan, that you have to comply with requests because your people in China will be arrested. As I understand it, Mr. Krumholtz's companies organized to have their people here in this area. Is that correct?

Mr. KRUMHOLTZ. No. We have employees in China, and our employees there face the same risk of not complying with a legally binding order as Mr. Callahan's would. The point I was making earlier is that our servers are located here in the United States, which adds an additional layer of process and protections through an international treaty between the United States and China on their ability to reach the content of e-mail traffic.

Mr. LEACH. And my understanding is Google has no storage in China. Is that correct?

Mr. SCHRAGE. We do not maintain any personally identifiable information in China.

Mr. LEACH. This is a profound distinction, as I understand it, because to go through our Government, you have to get the approval of our Government—is that correct?—for sharing information, which raises the Catch 22 for you at Yahoo!: Why did you put your servers in China?

Mr. CALLAHAN. To clarify, we no longer do have operational control over Yahoo! China. It is controlled by the company that we did a partnership with in October of last year. At the time when we did put our servers in China, we were the first western Internet company to be licensed to move into China in 1999. We made a decision at the time that the service that was available without having servers there, given the infrastructure of the Web at the time, going on 7 years ago, made the service not something that was robust and even took a while to maintain. So we made the decision to put the servers on the ground, and as you said, that is a distinction from the others that we just talked about.

Mr. LEACH. The irony of this distinction is that it puts you quite vulnerable to responding to requests that the other two companies do not to the same degree. Is that valid?

Mr. CALLAHAN. Yes. As to lawful requests for e-mail, as we discussed, that is correct.

Mr. LEACH. That raises a question of whether you want to continue that policy.

The second question, and it is a very interesting one, "lawful request" deserving of definition, and lawful requests in a Chinese context, should they be consistent with the Chinese Constitution, and do you ever question that? When the Chinese Constitution asserts freedom of expression, and an allegedly lawful request to repress freedom of expression, what is lawful? Do you have lawyers, and do you think this through? You are an attorney.

Mr. CALLAHAN. Yes, sir. As to your first question, we no longer operate the business there, so having servers there or not having servers there is not a decision that we would be in a position to make.

Mr. LEACH. So your prior suggestion that you had to do it because your employees would go to jail; you have no employees there. Which is the correct answer, that you have no employees, or you do have employees?

Mr. CALLAHAN. We do not have employees there. I was referring to the disclosure of information in the Shi Tao case which occurred when we did have employees there, so that was the distinction.

As to your question regarding the disclosure of information in other cases, I think, is what you were referring to, when we were operating there, we maintained very rigorous procedures to do that. We do have Chinese lawyers on the ground to make sure that these are lawful orders, that we are required to comply. There were situations when we did not comply, when we did not think it was a lawful order and not something we had to.

So I am confident that with those procedures in place that we tried to address that, recognizing your distinction between what is lawful in our context and in the Chinese context, that we did have to comply with the order.

Mr. LEACH. Well, I understand the corporate dilemma that is being expressed by the gentleman from Google. That is an understandable situation, but there is some use of words I want to understand here. You indicated that self-censorship was required, as I understand it, but it is my understanding that it was voluntarily undertaken, and you did not have negotiations with the Chinese Government. Is that valid or invalid?

Mr. SCHRAGE. Congressman, it is a condition of the license to do business in the country that you comply with the law, and it is a condition of complying with the law that you restrict the content available. So I do not believe we had much of a negotiation about that.

Mr. LEACH. So it is not true that you did this in anticipation of the Chinese Government objection. You had the government objection prior.

Mr. SCHRAGE. They would not give us the license if we did not agree to it. It is complying with the law. A condition was will you comply with the law, and we said yes.

Mr. LEACH. Did you affirm that the law existed and that the law was Constitutional?

Mr. SCHRAGE. I honestly do not know the processes we went through. I think it was made very clear to us that unless we would comply with the law as they interpreted it, we would not get the license.

Mr. LEACH. What I am getting at here is one of the traumatic aspects that the Chinese people are confronting today is that the Constitution provides certain very broad and thoughtful provisions on freedom. Many laws assert the same thing. And then there is this distinction between the Constitution and law but also the Constitution and law together, which are credible, but government officials are operating outside the Constitution and sometimes outside the law, yet they are official agencies of the government.

So the Chinese people are confronted every day with this perplexing circumstance, and one of the interesting questions is, does American corporate activity end up, through its policies, affirming outside of Constitution and, to some degree, outside of law actions, even though they are suggested by a formally structured government at some level or another? As a corporate actor, I think all of you are more or less general counsels. Do you think these issues true, and how do you assert the best interest of your company, and then is that best interest of your company the same as the values of the country from which you have your charters from? This is a dilemma.

I cannot tell you that it is an easy dilemma to answer. You have been very direct in asserting that you want to do business, and you are uncomfortable, but you want to do business, and that is an understandable circumstance, too. Whether it is a compelling one, individuals will have different judgments.

Mr. SCHRAGE. I would say two things. First, I would have to say, first and foremost, I am not the general counsel, so the general counsel would be very upset if I started giving legal opinions.

Secondly, though, you raise a very good point, and I would have to check it, and I would be happy to ask my colleagues to get back to you on the specific questions about what kind of legal analysis we performed. I would say, though, that there is some other empirical evidence, and that is there are lots of other companies that are doing search inside of China that have these same kinds of restrictions and self-censor or censor, and there are lots of Internet service providers, ISPs, as opposed to search providers, which perform filtering or censorship as well.

The only thing I would say is I do not think it would be correct to characterize this as sort of renegade bureaucrats in our situation. I think it is a government policy of complying with the law and interpreting the law in the manner that we have followed, but I would be happy to check it and get back to you on it.

Mr. LEACH. You have referenced that you are obligated to do all of these things because of a license. Did you have very specific terms in this license? I mean, did they cite exactly what it is you were to block in this license that you have, and then if it did not, how do you know what to block, if it is not that you are anticipating government actions? I mean, how do you know?

Mr. SCHRAGE. My understanding is, and, again, I do not have the license in front of me, but I did have a conversation with my colleagues about this very issue, the license makes reference to the

laws that need to be respected or complied with, and that is the basis.

Mr. LEACH. So you interpret these laws on specific things.

Mr. SCHRAGE. Based on the practices.

Mr. LEACH. Did you check with Yahoo!? How do you know what the practices are? Did you check with your competitors? They have to do this, so we are going to do this?

Mr. SCHRAGE. What we did was we set up a computer in China and started performing searches, and as the Chairman demonstrated rather powerfully, we learned from using other services and comparing the results of other services to our own——

Mr. LEACH. So you just put down what others did, for example, your Chinese competitor, and decided to do the same thing without being asked. That makes you a functionary of the Chinese Government. You have asked yourself the questions of what if I am a censor, what would I want to censor? You go to the practices of others, and then you follow them. Is that a valid description? This is an amazing description, I want to tell you. This is using your technology to learn how to censor.

Mr. BLUMENAUER. Will my friend yield for 10 seconds?

Mr. LEACH. Of course.

Mr. BLUMENAUER. What I heard earlier was that the Chinese system was built on what was available in China.

Mr. SCHRAGE. What was searchable.

Mr. BLUMENAUER. You operated in China based on what was available. That is what I heard you say in your original——

Mr. SCHRAGE. Let me be absolutely precise, and my colleague has explained that my earlier answer was not complete. What I said was correct in that we went into China and started performing searches to find information, both inside China and outside China, but the starting point was within China.

We did not only look at what our competitors did. We also sought to perform searches on our own search engine, google.com, from outside the restrictions imposed by the Chinese Government. So we would do many searches, many of the searches involving issues that are not controversial, not, as we are calling them, politically sensitive. They would yield all sorts of results. Many of the searches were the searches that are on categories that we are calling politically sensitive, when we performed those searches inside China seeking to go outside China, we were unable to get results outside China, but we were able to get some results, as in the example that the Chairman gave earlier, from within China.

So that result was not obtained by looking at the performance of our competitors but was looking at the performance of the filtering of government authorities.

Mr. LEACH. Well, this is very interesting. In all industries, we have all heard this term "best practices." I think you just have affirmed a novelty in American commerce, worst practices you have studied and adopted. That is an astonishing circumstance.

So if this Congress wanted to learn how to censor, we would go to you, the company that should symbolize the greatest freedom of information in the history of man. This is a profound story that is being told.

Mr. SCHRAGE. Congressman, I would make a couple of points.

Mr. LEACH. Of course.

Mr. SCHRAGE. First, I hope, as was clear from my testimony, both the written testimony that I submitted and the oral testimony that I gave, that this was not something that we did enthusiastically or not something that we are proud of at all.

Secondly, I think we are taking steps that others have not taken to, at the very least, make people inside of China and those outside of China aware of the detail and extent of the filtering that we are required to impose outside of China, through the kind of example that the Chairman documented, and inside China, by putting a statement at the bottom of every page of search results that are required to be filtered saying that we are not showing the full range of results because we are required not to as a result of government laws and restrictions. But you are absolutely right. It is what it is.

Mr. LEACH. Well, I appreciate this description. I appreciate the frankness of yourself and the panel. These are very difficult dilemmas that we face as a society and as people operating in commerce. How, as a country, we can respond is an interesting challenge. It raises big issues for all of us, and I thank you all very much.

Mr. SMITH OF NEW JERSEY. Mr. Faleomavaega?

Mr. FALEOMAVAEGA. Mr. Chairman, if I could, I would like to defer my time to our distinguished Ranking Member. I have all of the time in the world to ask our friends.

Mr. LANTOS. I thank my friend. I was here for the early part of the hearing, and I watched you on television in my office. I have a few very simple questions.

Mr. Schrage, you just indicated you are not proud, and you are not enthusiastic. Can you say in English that you are ashamed of what you and your company and the other companies have done?

Mr. SCHRAGE. Congressman, I actually cannot.

Mr. LANTOS. Cannot.

Mr. SCHRAGE. I cannot say that. As I alluded to earlier, I do not think it is fair to say that we are ashamed of what we have done.

Mr. LANTOS. I am not asking for fairness; I am asking for your judgment. You have nothing to be ashamed of.

Mr. SCHRAGE. I am not ashamed of it, and I am not proud of it. We have taken a path. We have begun a path, as I said in my testimony and in my written submission, we have begun a path that we believe will ultimately benefit our users in China. If we determine, Congressman, as a result of changes in circumstances or as a result of the implementation of the google.cn program service, that we are not achieving those results, then we will assess our performance, our ability to achieve the goals, and decide whether or not to remain in that market.

Mr. LANTOS. Let me ask your colleagues, beginning with you, sir, are you or is your company at all ashamed of what you have done in this whole business?

Mr. CHANDLER. We are not a service provider in China, and we do not have access to user information.

Mr. LANTOS. Just answer me directly. The totality of the things that you and the other three companies before us have done; are you proud of it, or are you ashamed of it?

Mr. CHANDLER. The products that we provide in China are identical to the products we provide worldwide with fundamental capa-

bilities that are necessary to operate networks. I think you very articulately and profoundly alluded in your opening statement this morning to the issue of appropriate ways of engaging in China. Every President since President Nixon of both parties has made a decision for engagement.

What we have done is followed very closely the policies of our Government, which are informed by human rights concerns and have been for 30 years now, in terms of determining what products are appropriate and not appropriate to provide to China and to which users, in keeping with what our national goals are with respect to engagement.

Mr. LANTOS. Taking the totality of your activities in China, there is nothing that you or your company need to be ashamed of. Is that your testimony?

Mr. CHANDLER. Our company provides Internet infrastructure——

Mr. LANTOS. I am asking a direct question. Is there anything that you have done in the whole period you operated in China that the company ought to be ashamed of?

Mr. CHANDLER. Our company provides access to information for people all over the world, including China, on a consistent global platform which maximizes the opportunity for freedom of expression, and we think that is a positive thing that we do throughout the world, including China.

Mr. LANTOS. So your answer is you have nothing to be ashamed of.

Mr. CHANDLER. My answer is I feel that our engagement is consistent with our Government's goals, and it is a positive engagement.

Mr. LANTOS. Let me move on to your colleagues. What is your answer, sir?

Mr. KRUMHOLTZ. We comply with legally binding orders, whether it is here in the United States or in China or in any of the other 90 countries where we do business.

Mr. LANTOS. Well, IBM complied with legal orders when they cooperated with Nazi Germany. Those were legal orders under the Nazi German system. Since you were not alive at that time, in retrospect, having a degree of objectivity which some of you are incapable of summoning up with respect to your own case, do you think that IBM, during that period, had something to be ashamed of?

Mr. KRUMHOLTZ. Congressman, we think that, on balance, the benefit of providing the services that Microsoft provides——

Mr. LANTOS. My question relates to IBM and Nazi Germany.

Mr. KRUMHOLTZ. I cannot speak to that.

Mr. LANTOS. You have no view on that.

Mr. KRUMHOLTZ. I am not familiar in detail with IBM's activities in that period.

Mr. LANTOS. Did you hear our Chairman's opening remarks on that subject?

Mr. KRUMHOLTZ. Yes, I did.

Mr. LANTOS. Do you think those are accurate remarks?

Mr. KRUMHOLTZ. I take the Chairman at his word, certainly.

Mr. LANTOS. I also take the Chairman at his word. Assuming that his words were accurate, is IBM to be ashamed of that action during that period?

Mr. KRUMHOLTZ. Congressman, I do not think it is my position to say whether or not IBM is to be ashamed of its action in that period.

Mr. LANTOS. How about you, sir?

Mr. CALLAHAN. As to Yahoo!, sir, we are very distressed by the consequences of having to comply with Chinese law. I spoke in my testimony that we condemn the persecution of any person for exercising their right to free expression. We are certainly troubled by that. We look forward to working with our peers and with the Subcommittee. The attention that is now on this issue, the initiative from the State Department, we think, is very encouraging, and we look forward to trying to push this issue forward as an industry collectively with government to try to make some progress.

Mr. LANTOS. Could I ask each of you, do you think that individuals or families have been negatively impacted by some of the activities which we have been told, like being in prison for 10 years? You are aware of those facts. I am talking to you, Mr. Chandler.

Mr. CHANDLER. I did not understand the question as it relates to individuals.

Mr. LANTOS. There are some Chinese individuals, not random individuals, the most courageous individuals in Chinese society, who stood up for the values we believe in in this country. Some of these people are in prison now. You are aware of that.

Mr. CHANDLER. Yes. I understand that, Congressman.

Mr. LANTOS. All four of you are aware of that. Have any of the companies reached out to these families and asked whether you can be of any help to them?

Mr. CALLAHAN. Congressman, we have expressed our strong views on this subject to the Chinese Government.

Mr. LANTOS. No. Have you reached out to the family offering assistance?

Mr. CALLAHAN. We have expressed our condemnation of the persecution of this person. We have expressed our views to the Chinese Government, and we believe the best way to engage this is a government-to-government issue.

Mr. LANTOS. Have you reached out to the family?

Mr. CALLAHAN. We have approached the Chinese Government on this issue, and we look forward to working with the United States——

Mr. LANTOS. Have you reached out to the family of the people who are currently in prison?

Mr. CALLAHAN. Congressman, we believe the best way to address this issue is to focus——

Mr. LANTOS. I can ask you 10 more times if you refuse to answer it. You are under oath. Have you reached out to the families?

Mr. CALLAHAN. We have not reached out to the families.

Mr. LANTOS. That was my question. Have you reached out to the families?

Mr. KRUMHOLTZ. Congressman, to my knowledge, none of the people involved in the, I believe, five cases where Microsoft has removed access to MSN Spaces in China, again, in response to a le-

gally binding order, involved anyone being incarcerated. So I am not aware of any families for us to reach out to.

Mr. LANTOS. Have the families been adversely affected?

Mr. KRUMHOLTZ. Not to my knowledge.

Mr. LANTOS. Well, have you explored? Have you taken the trouble? You have done a lot of work to prepare for this hearing because you are under pressure now. You wish this hearing had never taken place. We all understand that.

Have you reached out to the families that may have been adversely affected?

Mr. KRUMHOLTZ. With respect to the blogger whose content was taken down on December 30, who uses the pseudonym "Michael Anti," we returned his content to him because that was his intellectual property.

Mr. LANTOS. Have you reached out to his family and asked if you could be of some help because they may be under pressure?

Mr. KRUMHOLTZ. Not to my knowledge.

Mr. LANTOS. Not to your knowledge. How about you, sir?

Mr. SCHRAGE. Congressman, the best way we can honor——

Mr. LANTOS. I am asking you a direct question. I do not want your philosophy. Have you reached out to the families that have been adversely affected?

Mr. SCHRAGE. Congressman,——

Mr. LANTOS. Yes or no.

Mr. SCHRAGE. We do not offer a service that puts anyone in that situation, and the best way we can honor their situation is to ensure that we are not associated with a similar situation. We do not offer products that would put us in the position of putting people like that in danger.

Mr. CHANDLER. We are not a service provider in China. We do not have information regarding individual users of the Internet. We do not track individual users of the Internet. We have no access to any information or any relationship with individual users of the Internet.

Mr. LANTOS. I have heard a great deal of legalese, so let me pose a couple of hypotheticals. If you operate in a country which discriminates against women, like Saudi Arabia, for instance, would you comply with government orders which would compel you to discriminate?

Mr. CHANDLER. We do have operations in 50 different countries of the world, and I do not know what our human resources policies are in Saudi Arabia or elsewhere where there might be laws which treat men and women differently than we do in this country.

Mr. LANTOS. What would be your judgment? Would you comply, because I have now heard the words "complying with the law" ad nauseam and ad infinitum? If the local law compels you to discriminate between men and women, would your company do that?

Mr. CHANDLER. What I can do is provide you with information about what we actually do do in that respect in different countries of the world because different countries, including industrialized countries, have different standards for how men and women can be treated, different programs that have to be offered to men and women separately which are different than what we have in this country.

Mr. LANTOS. I am not talking about benefits. I am talking about discrimination. If a government compels you to discriminate against women, would your company comply?

Mr. CHANDLER. I do not know what types of requirements we are being asked to comply with.

Mr. LANTOS. It is a hypothetical question. If you were in a country where there is discrimination against women, and there was a legal requirement that obligated you to discriminate against women, would you comply with that provision of law?

Mr. CHANDLER. Well, I do not know what is meant by "discrimination." I am not trying to parse legalistically your question.

Mr. LANTOS. You are the only human being in the room who does not know what the word "discrimination" means.

Mr. CHANDLER. Well, it means different things in different countries, and there are different standards in France, in the United Kingdom, here, as well as in Saudi Arabia, and for that reason we do have policies in each of the countries where we operate, and I am happy to provide you a summary of those that will help inform a judgment of how we treat our people globally. We do operate in 50 different countries.

Mr. LANTOS. Mr. Schrage?

Mr. SCHRAGE. I am not sure how laws would require us to discriminate against women in the services that we offer. I do not believe we would comply with such a request. It is a hypothetical question, and you are asking me to sort of speculate about how discrimination relates to the kinds of services that we offer.

Mr. LANTOS. How about you, sir?

Mr. KRUMHOLTZ. Congressman, if we conclude that restrictions, either on our ability to provide services or our operations, are so stringent, there are many things that we will refuse to do, and we would back out of that market.

Mr. LANTOS. They would not be stringent. They would only be discriminatory. Would you participate in discriminatory policies?

Mr. KRUMHOLTZ. We have an antidiscrimination policy corporate-wide, so the answer would be no.

Mr. LANTOS. And that applies equally in every country.

Mr. KRUMHOLTZ. Yes, sir.

Mr. LANTOS. Even in countries where there is discrimination against women.

Mr. KRUMHOLTZ. Again, if the discriminatory restrictions are such that they adversely affect our ability to operate in that country or to provide our services to our customers, we would consider backing away from that country.

Mr. LANTOS. How about you, Mr. Callahan?

Mr. CALLAHAN. Congressman, I also do not think it would be appropriate for me to speculate as to how a hypothetical would apply to our services or not. However, I will say that we have been very up front about the fact that our compliance with Chinese law in this case has caused very serious consequences, and it is one that we look forward to trying to find a way to address as an industry.

Mr. LANTOS. Would you have come up with the new statement of principles had it not been for this congressional inquiry?

Mr. KRUMHOLTZ. Is that directed in terms of our new blogging principles?

Mr. LANTOS. Yes.

Mr. KRUMHOLTZ. Actually, we were very distressed by the take-down request that we felt compelled to comply with on December 30 of last year. As a result of that take-down request, we launched an internal review of what our procedures were, what was in place in that instance, and what could we do to improve them. Hence, that was what drove the new policy.

Mr. LANTOS. Thank you, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. Thank you, Mr. Lantos.

Mr. Pomeroy? Blumenauer?

Mr. BLUMENAUER. Thank you, Mr. Chairman. I appreciate very much the gist of the testimony that has been offered up here. I think you have been able to identify that each company has different services and different circumstances, and I think you have helped me understand that just asking the same question to each of you actually would produce different responses because you have different business models, different product lines, different services, and I think that is very important to have part of the record, and I hope as this sort of settles down a little bit and as we sift through it, we understand that Microsoft, Google, Cisco, you are discrete businesses involved with different activities, and I appreciate having that clarified.

I think you have also endured a great deal right now, and there are other people on the Committee who want to engage in a discussion, which I do think is very useful, but if we could, because you are each discrete enterprises, different business models, different practices, different requirements, I would like to get a sense of what your competitors are. Are you unique? Is there any choice as far as China is concerned, where you have unique leverage, that they either deal with you, or they are at some serious disadvantage? Mr. Chandler, if you want to start.

Mr. CHANDLER. Sure. Thank you, Congressman. In his opening remarks, Chairman Smith alluded to a tender in China where Cisco's products—he said four out of six contracts were awarded to Cisco and another American company, and there were, I think, two portions of that that I believe were awarded to a Chinese company as well.

In every single market space that we operate in we have vigorous competitors in the routing and switching markets that a lot of the discussion about URL filtering and the capabilities of our products in that regard for network management, there are probably at least a dozen companies worldwide that supply at least some segments of that, including very aggressive and hard-charging Chinese companies that are in the marketplace as well. It is a very competitive market for us not only in China but around the world.

Mr. BLUMENAUER. Thank you.

Mr. SCHRAGE. We have several lines of business. Some of our lines of business overlap and compete with my colleagues to my left. Some of them do not. In China, as I mentioned earlier on, we have particular challenges with local competition and, in particular, one local competitor whose dominance in the market is actually much, much greater than our market power.

Mr. KRUMHOLTZ. We, too, have several lines of business, many of which we are engaged in China, and there are competitors across all of those lines. I mentioned in my written statement and, I think, in my oral statement as well that with respect to MSN Spaces, our personal Web site or blog service, there are a number of Chinese competitors. As a software provider, probably our greatest competitor is the extraordinarily high piracy rate in China which is, I believe, still over 90 percent despite the very excellent work done by our own Government to advance our industry's agenda in that regard.

Mr. CALLAHAN. Through Yahoo! China, when we operated the company, which is now operated by Alibaba, we provided search services, communications, and e-commerce services. Now that form takes the Yahoo! China division of Alibaba of which we are a shareholder and a board member.

Mr. BLUMENAUER. Are there direct competitors with Yahoo!/ Alibaba in those areas?

Mr. CALLAHAN. Yes, there are. The competition here, of course, the local competition in search and communications, and, I believe, an eBay substantially in China as well.

Mr. BLUMENAUER. Thank you. My sense is, just in listening to your testimony, that there are upwards of 100 different countries around the world where you collectively do business in many of the larger countries you probably all are engaged, and you are subjected to a wide variety of local laws, rules, and regulations, and you referenced Microsoft's interest in piracy, the rules of the game, something that a number of people on this Committee are deeply concerned about, not just intellectual property but a whole range of areas.

As a matter of course, do you drill down into the rules and regulations, the Constitutions of the various 100 countries to try and find out are they consistent with their Constitution? Do you do a separate legal interpretation of all of the rules and regulations that you are required to abide by, or do you assume, like in the 50 states, that the people who are in charge more or less know the rules of the game, and you abide by them? I just wonder because there is a hint here of: "Maybe this isn't Constitutional. Is there a conflict with other provisions of Chinese law?" How do you operate in the 100 countries?

Mr. SCHRAGE. We have a big legal department that is not that big. As a practical matter, when we hear from government officials about how they define the laws and what they define compliance to mean, we generally accept that.

Mr. BLUMENAUER. Germany, Great Britain, Seattle?

Mr. SCHRAGE. All of those.

Mr. BLUMENAUER. Do any of you do anything any different? Are you aware of anybody that does any different?

Mr. CALLAHAN. Congressman, where we have local operations we do have in most of those places attorneys on the ground that would do the local legal evaluation. They work as members of my department, and we would comply with laws as we are required to.

Mr. BLUMENAUER. I am interested if the notion of censorship ought to be pursued through our U.S. trade representative as a

barrier to trade. Is that something that should be pulled out and discussed separately? Would that be helpful? Is that possible?

Mr. SCHRAGE. We have certainly indicated, as I indicated in my written testimony, that we think that that would be a conversation worth pursuing, again, not necessarily just with respect to China but as an issue around the world.

Mr. CALLAHAN. We think that there is a real opportunity, given the highlight on this issue, from the attention of the Subcommittee and the hearing that was called by the Chairman, the interest from the State Department, and the interest among the companies here, as well as broadening this issue to not just be about the Internet but make it about media and telecom. We think that, given the groundswell of particularly public interest in zeroing in on the issue itself, there is an opportunity here for government and industry to cooperate together and try to make some progress, so we are encouraged by that. Certainly, censorship is one of the issues as well.

Mr. BLUMENAUER. Mr. Chairman, I appreciate your courtesy and our Ranking Member's courtesy to me. This was very instructive. I think I have learned a lot just as a result of the testimony, the vigorous questioning, and I am looking forward to where we go from here to try and take difficult questions, elaborate on them, look at ways that we can make contributions. But I think just this hearing has provided, I think, an important contribution to deal with the serious issues that you have raised, and I appreciate it.

Mr. SMITH OF NEW JERSEY. Thank you, Mr. Blumenauer. Thank you for your work on this. We will share—as a matter of fact, we have already shared, and hopefully your office has it—the text of our draft bill, and obviously it is a work in progress, so we look forward to your input.

Chairman Burton?

Mr. BURTON. Thank you, Mr. Chairman, and thank you, gentlemen, for being here today. I appreciate it.

You know about the Golden Shield being used as a tool to not just improve police efficiency but to monitor Chinese civilians, and if they say or do anything acrimonious or opposing the government, they put them in jail for a long time. What I would like to know is if you were not involved over there, would other domestic companies over there be able to do the same job that you are doing?

Mr. CALLAHAN. Congressman, from Yahoo!'s part, we no longer operate a company on a day-to-day basis there, but the services that we provided at the time we believed to be very comprehensive, robust, and of a better quality than the local competition.

To answer your question directly, and the other representative asked it as well, there are direct competitors in the search, e-mail, communications, and e-commerce platforms——

Mr. BURTON. What I am trying to get at is I have been reading in the paper about how American companies are over there assisting the government in keeping a clamp on people who are dissidents and people who oppose things that are going on in the government. What I am trying to get at is if Microsoft, if Yahoo!, if Google, if all of you had not been over there, would this have taken place anyhow, and could they have done it in as efficient a way as they have done it? You know the capabilities of your company. I

am just asking you, could it have been done by a local or domestic company over there or companies?

Mr. SCHRAGE. Congressman, we did not enter the market until just recently, and part of the reason we entered was because other people were doing it, and so we, as a competitive reason as well as for the other reasons I have outlined, that is why we made the difficult decision we have made. So, yes, there are other competitors who claim to do precisely what we do. We do not think they do it as well as we will, and we think we will win as a competitive matter, but the market would continue and would grow whether we are there or not.

Mr. BURTON. What do you think the answer is, because you, like all of us, believe in freedom of speech and free enterprise and the ability of people to live under democratic institutions? What do you think about your products being utilized by the Communist government over there to enforce the police state? What do you think about that?

Mr. SCHRAGE. As I hope I made clear in my testimony, we are not happy about it at all, and that is one of the reasons why we think it is a great idea to have joint industry action and an as good, if not even better, idea for us to work with the State Department and the Congress to find ways to help us.

Mr. BURTON. Are you, as an industry, working together to try to find the solution to this problem so that you are not perceived that way?

Mr. SCHRAGE. I think those efforts have begun. I feel confident they will accelerate. We will see where they go, but we see the need, and we are hearing you and your colleagues loud and clear.

Mr. BURTON. Okay. There is a bill that was introduced by Representative Cox—I am sure you are familiar with it—H.R. 2216, which would authorize $50 million to develop and implement a global Internet freedom policy, combat state-sponsored and state-directed Internet jamming, repressive foreign governments such as the PRC, and the intimidation and persecutions by such governments of the citizens who use the Internet.

I presume, since you guys are going to be talking to each other about this, you will be working with us to try to get something like that passed through the Congress that would allow people a modicum of freedom in using the Internet in those countries.

Do any of you have any outreach programs for people or educational programs for people in China in communities over there?

Mr. KRUMHOLTZ. We have a program—actually it is a global program—I am speaking for Microsoft, Congressman—called Unlimited Potential in which we are going into countries all over the world—we operate in 90 countries, as I testified earlier—and establishing community technology learning centers and providing underserved populations the ability to get basic IT skills training. So we have a number of projects in China.

Mr. BURTON. Have you read Congressman Smith's draft bill called the Global Online Freedom Act of 2006? Have you had a chance to look at that?

Mr. KRUMHOLTZ. I have not.

Mr. BURTON. I wish you would. Mr. Chairman, could you give a copy of that to all of them so they could take a look at it and see

if there are any additions or deletions that you would like to see in that act that would help us in our work to help solve this problem?

I think I have one more question, Mr. Chairman.

Have you any kind of counter-censorship software that is currently in production or could be used by people in countries with repressive regimes that they could use right now, counter-censorship software? I am sure you know what I am talking about. Do any of you have anything like that that could be used or distributed or purchased?

Mr. KRUMHOLTZ. Not that I am aware of.

Mr. CALLAHAN. No, sir, not Yahoo!.

Mr. BURTON. Any of you? Could that be developed? I do not have the technology skills that you guys have. It seems to me, if you can come up with a program like you have, you could come up with one that would countermand that or counteract that. Would that be possible?

Mr. CHANDLER. There are a number of efforts underway, Congressman, and I think Chairman Smith alluded to several of them in his opening statement, that are assisting people in evading censorship. The key to being able to nourish those programs and support them will be having an Internet that operates globally on one standard. Efforts such as the Chinese undertook a year ago to set up their own standard for some Internet access devices only allow Chinese companies to manufacture them, which our Government pushed back very aggressively and so far successfully, although we anticipate it will come back.

Maintaining that one global standard will be essential to allowing those efforts that are going on to succeed, and there are a number of them. One was highlighted in the *Wall Street Journal* just this past Monday called "Freegate" in North Carolina. There is an effort out of Harvard. There is one at the University of Oregon and Cal-Berkeley as well. So there is a lot of that activity happening, and its success will depend on having a standardized Internet globally, and that is a key interest of ours in maintaining an open Internet.

Mr. BURTON. Well, I appreciate very much you fellows coming here today. I know you probably approached this hearing with a great deal of trepidation, but if you are willing to work with us, I am sure the Congress wants to work with you to help solve this problem. I cannot believe that those of you who have made your millions in the free enterprise system would like to see a repressive government like that to take your tools and use them to repress their own people. So, hopefully, we will work together to help solve this problem, and thank you very much for being here.

Mr. SMITH OF NEW JERSEY. Mr. Faleomavaega?

Mr. FALEOMAVAEGA. Thank you, Mr. Chairman. I was taking circles over here from Mr. Krumholtz's testimony saying that Microsoft currently operates in 90 countries.

Mr. KRUMHOLTZ. Yes.

Mr. FALEOMAVAEGA. And I believe also Mr. Chandler mentioned that Cisco operates in 50 countries.

Mr. CHANDLER. Approximately, yes.

Mr. FALEOMAVAEGA. Approximately 50, give or take 5. And, Mr. Schrage, I did not get the number of countries that you operate, Google does.

Mr. SCHRAGE. Wherever there is a computer and an Internet connection, you can probably reach Google, so you tell me how many places that is, and that is how many places——

Mr. FALEOMAVAEGA. Can you kind of wing it, an approximate number of countries that Google is——

Mr. SCHRAGE. I think it is probably around 100 countries.

Mr. FALEOMAVAEGA. A hundred countries? How about Mr. Callahan with Yahoo!? How many countries do you operate under?

Mr. CALLAHAN. Anywhere you could reach Google, you could reach Yahoo! as well.

Mr. FALEOMAVAEGA. So it is 100 countries as well.

Mr. CALLAHAN. We have operations in just over 20 countries.

Mr. FALEOMAVAEGA. Twenty?

Mr. CALLAHAN. Yes.

Mr. FALEOMAVAEGA. I thought you had more than that.

Well, gentlemen, welcome to the lion's den. I am sure that this is probably the first time that you have had to appear before a congressional Committee, and I wanted you to know the tremendous sensitivity that Members of this Committee have, and I would like to note for the record that in the years that I have served as a Member of this Committee I cannot say more and have the highest and utmost respect for the Chairman of our Subcommittee not only myself as a member of the Human Rights Caucus, but in the years that he has served on this Committee, he certainly has my respect in expressing the same concern to countries that we deal with. I am absolutely certain that what we are trying to pursue here is to make sure that our companies doing business in other countries of the world have that same sense of sensitivity and understanding of freedom and what democracy is all about.

In the announcement that was made by Secretary Rice about the formation of this Global Internet Task Force, it is always nice to make announcements and say that the State Department or the Administration is going to look into this problem, and I wanted to ask you gentlemen, is the Administration really serious about addressing the issues that the Chairman and the Members of the Committee have brought to your attention in terms of having to deal with a country like China?

My reason for asking how many other countries you deal with—in what other countries have you encountered similar situations where there are serious questions of censorship and prohibitions, the very example that you cited, Mr. Callahan, about Shi Tao? I am curious. Is this the first time that you have encountered this kind of situation with the Chinese Government, or have you encountered similar situations with other countries as well? I would like to have your comment on that.

Mr. CALLAHAN. For Yahoo!, the Chinese situation and the Shi Tao case are certainly unique.

I would say that as to your question about the State Department initiative, we applaud that, embrace it, think it is headed in the right direction. We think that help from the Executive Branch to help all the companies realize the full potential that our peers in

other companies in media and telecom could offer to push forward free expression is an important initiative. We think that American companies offer a unique combination of modernization and technology, and there could be a very compelling opportunity to move forward with that.

Mr. FALEOMAVAEGA. Mr. Krumholtz?

Mr. KRUMHOLTZ. With respect to the State Department initiative, we also applaud it. We think that it is going to be critical for both industry, the State Department, the Congress, and certainly the NGO community, too, which has a very important voice on these issues and a great deal of expertise, to come together to try to arrive at—the term "best practices" was used earlier, principles that could help guide United States corporations in how they do business not only in China but in other countries as well, going to your point about restrictive regimes or repressive regimes in other countries. I will say, I think, from our experience, China does present a special case and a particular challenge.

Mr. FALEOMAVAEGA. Mr. Schrage?

Mr. SCHRAGE. I really would just echo the comments that were just made. I think we think, again, based on the earlier panel, that the State Department is serious about it, and we are, too. We hope that together we can do something meaningful.

Mr. FALEOMAVAEGA. Mr. Chandler?

Mr. CHANDLER. Because we sell the same equipment with respect to the URL filtering capabilities we were discussing globally, and the filtering technology is a fundamental part of network management, we do not see as a company the implementation that is done by the user. We certainly have seen information that suggests there are a number of countries around the world that do perform filtering for political reasons as opposed to the technical reasons and network security reasons that we design the features.

Mr. FALEOMAVAEGA. The compliments that I had offered earlier in my statement saying that the one thing the Chinese Government is very sensitive about is, through the Internet, is pornography and gambling of a sort. I wondered, just to be curious, do you keep tabs of these types of things that come in through the Internet in China? How do you do the filtering process? Is there some kind of a standard or measuring device that you have to do this in order to comply with the Chinese requirements?

Mr. KRUMHOLTZ. Congressman, with respect to MSN Spaces, our blogging service in China, we respond to requests by Chinese authorities, legally binding requests, to take down content. You mentioned pornography. It so happens that we received a request from Chinese authorities just last week to take down a blog. When we went to examine the case, it turned out that it was not anything about political speech but about pornography, which actually, under our own terms of use, we would have also, if we had identified it before being told about it, would have taken it down.

Mr. FALEOMAVAEGA. Mr. Callahan?

Mr. CALLAHAN. I cannot speak to the current operations of Yahoo! China, as I mentioned, but when we did operate the business, similar to Mr. Krumholtz, Yahoo! would respond to notices to take down content in a similar fashion.

Mr. FALEOMAVAEGA. I think, if I might add to the course of the hearing this afternoon in terms of the tremendous problems that we are faced with in a country like China, as I am sure that the next panel that will be testifying before the Committee, it is not easy, and it is like a Catch 22 here. We are faced with a country that is growing economically with a tremendous potential as to why it is such an attractive market for just about every democratic country or the industrialized nations that want to invest and be present there, and I am sure that is the very reason why you are there also and your respective companies.

I remember noting that it took United Airlines about 15 years even just to get to Japan. I am sure that you must have had the same problems in trying to get access to the market or even get licensing. Since Google seems to be the last one that has gone in there, how long did it take you to get your license?

Mr. SCHRAGE. You know, I do not exactly know when the application was made, but we began the process of deciding whether or not we would do business within China, I would say, more than a year ago. So the whole process, from the time we really began to look at it seriously until the time we got the license and indicated we would launch the service, was well over a year.

Mr. CHANDLER. We have been active in China since 1994 in providing Internet access equipment.

Mr. KRUMHOLTZ. We have also been active in China since the mid-1990s.

Mr. CALLAHAN. We first established operations there in 1999 and then went to a strategic partnership where we were an investor in 2005.

Mr. FALEOMAVAEGA. So, gentlemen, you are pretty much aware, then, of the situation in terms of our not only diplomatic relationship with China but in every aspect of trade and commerce, but do I sense a consensus among our four big corporations' presence in China the sensitivity that we have here in this Committee to see? I think the bottom line, as I note here in my notes, is censorship, and that if it affects the lives of the people in China and how you deal with on a commercial basis, I think this is where the rubber hits the road—is that how you say it?—and I sincerely hope that not only will we be working with the Global Internet Task Force, but the fact that Chairman Smith has proposed a draft bill, we certainly will welcome your input and see where we need to go from there.

Thank you, Mr. Chairman, and thank you, members of the panel.

Mr. SMITH OF NEW JERSEY. Thank you very much.

Mr. Rohrabacher? Chairman Rohrabacher?

Mr. WEXLER. I thank Mr. Rohrabacher for yielding. I very much appreciate that. I would like to associate myself with Mr. Faleomavaega's opening remarks wherein he complimented the Chairman. No one has a finer record on these issues than Congressman Smith.

I would like to offer—I think I have listened to most of the hearing—a different view. Congressman Lantos asked the question, should IBM be ashamed to the degree they were complicit with the carrying out of the Final Solution during the regime of Nazi Ger-

many? Quite frankly, it is an easy answer. The answer is yes. IBM should be ashamed.

But there is also another question that should be asked, and it should not be limited to IBM, if we are going to be fair. The question is, should we be ashamed that the United States Government did not do certain things that it could have done that would have dramatically affected the ability of Nazi Germany to prosecute the Final Solution? Yes, the United States Government could have bombed tracks leading to extermination camps. Yes, the United States Government could have made a different choice to bomb concentration camps.

I only bring that up because, in listening to this intercourse and this interaction, I think I agree with 100 percent of what has been said by the Members and asked of the witnesses. But there is one major gap here. We are not asking the same question after we asked them, not IBM but Microsoft and Yahoo! and whatever, are you ashamed? We should be asking, are we ashamed of the United States Congress? Are we ashamed of what the United States Government has done? Let us at least be candid and not be duplicitous.

The United States Government has far more tools at its discretion than does even these important companies. This Congress, most recently—now I disagree with it, and I know that there are members on this panel that disagree with it, but the United States Congress, speaking for the American people, gave up our biggest tool. We gave China most favored trading status, and the President signed it. If we are serious about human rights, if we want human rights to be the be all and end all, then do not give China most favored trading status.

If you go back in time, we should still have recognized Taiwan, not China. Now, I am not advocating for any of these measures, but my point is it is somewhat duplicitous of a government which has all of the tools, let alone, the American Government, the most powerful Government in the world, to then pinpoint a judgment call that corporations have made. And in effect, what we are saying, and it is a legitimate position, what, in effect, we may be saying is that X corporation should prioritize the issue of human rights and the consequences that an adverse government might take as a result of using their technologies, prioritize that interest versus the interest of their shareholders, the interest of their employees, the interest of their responsibility as a corporate citizen, prioritize that and refuse to do business in China.

Now, that might be a legitimate position for us to take. That may be a legitimate position, but if we are going to take that position, then let us at least have the consistency to say that trade for the entire country, the hundreds of billions of dollars that are related to it, is not as important as human rights. Let us do what we can do to dramatically affect human rights.

I would venture to say that the Chinese Government, if the Congress of the United States passed a law that said trading status will be affected if you, Chinese Government, continue to do what you are doing in terms of free speech and the consequences of them exercising it or not exercising it, that will have a far bigger impact than Microsoft saying, I am picking up my marbles and going away.

Mr. Chairman, I think this is probably the most profound hearing I have sat through, and I thought Mr. Leach's questioning and the interaction, to me, that is textbook for what this Congress should be doing, and I applaud it. But to me, the obvious consequence of this entire interaction is not necessarily an examination of what they do, but it is what we can do to affect positively the behavior of the Chinese Government in a way in which we will not have to worry about how they choose to interact with companies like this.

They are in a no-win situation, these companies. I do not know if I agree or disagree with the way in which they have behaved. I honestly do not know, but, and I will stop with this, Mr. Chairman, the *Washington Times* today—I think the best thing I have ever seen written in the *Washington Times* on their editorial page, last paragraph: No one should even want tech companies to try to decide which government policies are legitimate or dictate what the Chinese leaders should do to promote development of democracy. Advocate and advise, fine; boycott, no.

They are right. Do we want to hand over the reins of government to these guys? They have been elected by no one, with all due respect. They are great business people. We have been elected to make the fine distinctions between morality and trade and whether or not we want China's vote on Iran and whether we need their cooperation on North Korea, and we are supposed to balance all of that, but these business people are not supposed to balance it.

Thank you, Mr. Chairman, for giving me the time, and I think there is one issue that it will be quick to ask because I think, to a degree, it goes to the heart of what we are talking about in terms of their leverage. There was reference made to a fifth company, which I said is a Chinese company, and if there is a fifth company, which I presume that there is, could someone quickly, because I have used a lot of time, and I apologize, could someone describe what they believe reasonably would be the consequences of you four companies, and it is somewhat ironic—we must laugh at ourselves, and I respect Mr. Payne enormously, but when Mr. Payne starts talking about the consequences of antitrust behavior and essentially advocating that these companies get together and engage in that kind of behavior, it is ironic that we are doing it with a member of Microsoft on this panel that, you know, for right or wrong, was the recipient of all of this.

Could somebody tell us, if the four of you got together, not in violation of antitrust laws, and tomorrow said, we are packing our bags, what do you reasonably believe would be the consequences to the development of the Internet in China? Would these poor victims of the Chinese policy of this type of persecution, do you think they would be any better off?

Mr. SCHRAGE. I think that there would be less information, less available to people in China.

Mr. KRUMHOLTZ. I believe it would be a lose-lose. I believe that Chinese citizens would lose, and I believe that all of those of us who would like to promote greater democracy, greater freedom of expression in China would also be at a loss.

Mr. CALLAHAN. I would agree that the innovation and the open communication and ability to access all sorts of information would be restricted.

Mr. CHANDLER. We have vigorous competitors among Chinese companies and other non-American companies, as well as other United States-based companies. A withdrawal of companies that were committed to building an Internet based on global standards from China would have the effect of potential balkanization of the Internet and a closing down of information availability rather than an expansion of it.

Mr. WEXLER. Thank you. Mr. Chairman, if I could have 20 more seconds. I think this hearing points out maybe better than any other the nuanced interests and policies that we have as a people and a nation with the country of China and their people. What I think this hearing points out is that for every advantage, there may be a disadvantage, and we need to act very carefully and cautiously when we try to determine what we think will be consequences in China. That is the role of the government.

I do not think that is the role that we should try to engage companies to do to substitute for our judgment. They have their responsibilities as corporate citizens. They have their responsibilities to their shareholders for the safety of their employees. We pass laws to encourage them to behave in certain ways, but when they are acting pursuant to our laws and doing what they legitimately do as business, this hearing is fabulous in terms of information, but I would not want to see us pass the buck to them and not take those hard responsibilities ourselves. Thank you very much, Mr. Chairman.

Mr. ROHRABACHER. Mr. Wexler, I am happy that I was able to yield my time to you and now I have my own time. I think you have made some important points, but I do believe that there is a fundamental flaw in your logic.

Mr. WEXLER. There usually is.

Mr. ROHRABACHER. No, I would not say that. We agree on many, many things and the two of us have worked on many issues, but in terms of this issue, I think it is important for the public to recognize that when you suggest that these companies should not be out there having to make these decisions on their own and set these standards on their own, that is our job and that Congress has failed, there is another dimension to that, there is another layer to that onion.

Who do you think has been pressuring Congress to establish this opening so that big business can rape the people of China?

Who do you think has been setting up the think tanks in this city with their excess profits from dealing with dictatorships?

It is big business. Come on. I am a Republican, I am not supposed to be against big business. You are the guys who are supposed to be saying this, not me. It is clear as a bell.

The companies that are doing business in China, they are making huge profits off their dealings with this dictatorship and they take a portion of those profits to try to influence what Congress does or does not do.

Most favored nation status? Who lobbied for that? The corporations lobbied for that. Of course they did.

Yes, we do have a responsibility. We in Congress have a responsibility to set the standards. You are right. These corporations should not be the ones setting the standards for the American people, but they have been doing it. They have been doing it by influencing us directly and by trying to influence public opinion by setting up these foundations and think tanks. We documented that yesterday at a hearing of my Subcommittee on Oversight and Investigations.

So, no, we cannot let these guys off the hook because they are on the hook. They are not like doing business with dictators, but they are trying to influence government policy in a way that will permit them to continue to do business with dictators. Corporations are not interested in the well being of the people of China or any other country, but let us do our job, let us think about it and try to set up a system in which these fellows cannot make decisions that are going to help the police departments of a dictatorship, which leads me to my first question of you, Mr. Chandler.

Does your corporation differentiate at all between dictatorships and democratic governments in terms of whether or not you are willing to be involved with them in setting up systems that help police departments?

Mr. CHANDLER. We do in accordance with the principles that you have established for us. For 30 years, the discussion has gone on in this country and, as we have seen today, there were different opinions within the United States Congress on what the nature of that engagement with China should be. Certainly——

Mr. ROHRABACHER. How about other dictatorships?

Mr. CHANDLER. Certainly——

Mr. ROHRABACHER. How about other dictatorships? Let us forget China. You re right. Here we are, this Congress, because we have not set—I have been a long advocate of a dual process and dual standards for corporations doing business overseas: One standard for countries that are dictatorships and other standards for democracies. We have not done this, but do you do that with any dictatorships? Have you established any—not just what we have done in China, but what we do throughout the world?

Mr. CHANDLER. Well, I would start by saying I think some people have alluded to question about events 60 years ago and I think we have moved to a very different place from a time when American companies and Americans policy could turn a blind eye to repression, persecution and genocide. For 30 years, we have been bringing human rights concerns into our lawmaking about where United States companies should engage, how they should engage, not just with respect to China, but with other repressive regimes around the world.

Mr. ROHRABACHER. Let note that I think you are absolutely wrong. I have been around here 18 years, I worked at the White House 7 years before that. Your analysis is absolutely wrong. No, we have not tried to rein in our corporations in doing business in dictatorships. The only time we have been able to do that is when it is a direct threat to the United States security, but it has nothing to do with those moral positions at the basis of our society of life, liberty and the pursuit of happiness or any of these rights of

religion and other things that we hold dear as a people. Our Government has done a rotten job of that.

Mr. CHANDLER. Well, what we have to comply with, however, are regulations put in place pursuant to laws that the Congress has passed which do restrict where our products can be sold and who they can be sold to on concerns that include national security and human rights concerns and we do comply with those.

Mr. ROHRABACHER. And in China, how has that hindered, for example, the requests from police and national police in China with your company?

Mr. CHANDLER. Well, there are certainly some agencies of the Chinese Government that we are prohibited to provide our products to. There are other agencies which require a lengthy licensing process where the government makes a determination as to whether it is appropriate to supply products or not and we comply with those.

Mr. ROHRABACHER. How about the police? Is the police one of those?

Mr. CHANDLER. There are very stringent restrictions on equipment that is considered crime control equipment under the Foreign Relations Authorization Act that was enacted after the Tiananmen Square incident because of our country's reaction to what happened at that time. For some equipment, there could be restrictions. For other equipment, there are not restrictions. The law makes differentiations between different types of equipment and uses.

Mr. ROHRABACHER. Okay. So if we have any complaint about that in terms of your interaction with the police in China, we will just use China because that is what we are discussing, but there are other dictatorships in the world, that we should actually not be coming to you crying, but we should be basically just trying to reset the restrictions and make them tighter if we think they are too loose.

Mr. CHANDLER. Well, I think as an economy that is built around a private sector that carries out economic activity, we carry out our activity mindful of the rules that you set and the responsibilities that come from the system that we have and I think that is a reasonable way to approach that issue.

We believe that our products are a force for providing information around the world and empowerment and enlightenment to people and that is the effect that our products have had in countries all over the world.

Mr. ROHRABACHER. And you do not see that your company has ever lobbied Congress to try to establish what those rules were?

Mr. CHANDLER. We have not lobbied Congress on export control rules. We make administrative appeals from time to time to make sure the rules are properly implemented, but we have not lobbied, at least to my knowledge, at any time on the export control regulations with the U.S. Congress.

Mr. ROHRABACHER. Well, I heard your caveat there. We call them weasel words here, "to my knowledge, we have not," but I am sure somebody will be listening today and if your company has indeed lobbied in order to loosen the restrictions or change the restrictions, I am sure we will find out about that.

Mr. CHANDLER. I am confident I will hear that as well, Congressman. Thank you.

Mr. ROHRABACHER. All right. Okay.

Again, let me apologize that this happened to be one of the days that I had to meet with the President's Science Advisor, Mr. Marburger, so I have been deeply involved in other technology issues, but it is clear that we have had high technology companies suggesting that if we just open up and do more business with China that there is going to be a liberalization, we are going to find a more democratic and open society at the end of this interaction, and now we come to a point that we see high tech companies strengthening China's police force, even after there has been no liberalization, but in fact there has been a worsening of certain restrictions, especially on religious people and Falon Gong, for example.

Do you not think that that is sort of a reason for concern, I would leave that up to the whole panel, everything we have been told about how things are going to get better if we just deal more openly, have more economic interaction, and now we are reaching a higher stage of technology and we are finding the technology being used by the police state against the people, rather than liberalizing the society?

Your contention is with more information out there things are going to get better, but yet at the same time you have a fellow at the end of the table who is selling the technology capabilities of his company to strengthen the police that are controlled by the dictatorship. Does that not seem a little contradictory to you?

Okay. I will leave it at that.

Mr. Chairman, I gladly co-sponsor your legislation on this and congratulate you for holding this hearing.

Mr. SMITH OF NEW JERSEY. Thank you very much, Chairman Rohrabacher.

Mr. Sherman?

Mr. SHERMAN. Thank you, Mr. Chairman.

I am going to focus on the privacy part of this, the other part being the censorship part. I hope I have enough time left over to get into that.

Mr. Callahan, I am a Yahoo! customer. I have a lot of e-mails up there and they are all domestic. Let us say that you get a call from the NSA saying they want you to give them a copy of all my e-mails that are stored in Yahoo!, I have them going back 2 or 3 years, because they think that is important to the war on terrorism.

I am relying on your privacy policy. Can I rely on that privacy policy, that you are not going to give those e-mails to the NSA unless you get a court order?

Mr. CALLAHAN. Congressman, we do, of course, have a privacy policy, which, as you know, says that we will disclose information to law enforcement when required to. We do have a policy where we do not comment on specific law enforcement interactions, but I will say this——

Mr. SHERMAN. This has not happened yet, I hope, so this is not a specific ongoing investigation.

Mr. CALLAHAN. If you could let me finish?

Mr. SHERMAN. I am not high on the list of al-Qaeda operatives. Go on.

Mr. CALLAHAN. We would only disclose information in compliance with law and with our privacy policy.

Mr. SHERMAN. Compliance with law. Mr. Rohrabacher was talking weasel words a little bit. Court order or letter from the NSA?

Mr. CALLAHAN. It would be in compliance with law, sir. I would not be able to comment on whether——

Mr. SHERMAN. So if, for example, in its most broadly defined description of the power of the executive, the Attorney General says that the Executive Branch, without any okay from either of the other two branches, has a right to read absolutely everything you have in your files about me, you might very well agree and turn my stuff over without a court order?

Mr. CALLAHAN. It would not be appropriate for me to comment on whether certain action was authorized——

Mr. SHERMAN. Well, how am I supposed to be a user of Yahoo! if you will not tell me whether I can rely on privacy except by saying, well, we will decide later whether a e-mail from a sheriff in some obscure county says, "I hate Brad Sherman, I want information about him, I think he is a terrorist," you might turn it over.

Mr. CALLAHAN. You absolutely can rely on Yahoo!'s privacy policy and we would only furnish information if it was in compliance with law.

Mr. SHERMAN. You are their chief lawyer and you cannot tell me now that it is not compliance with law to provide all of my data to an investigation from some county, a sheriff of a county that I have never been to.

Mr. CALLAHAN. Sir, in the example that you give, if we were served with proper legal process and we were required to furnish that information, we would have to give it, but we would not provide it unless we were required to.

Mr. SHERMAN. Sir, you are assuming the answer to the question and pretending that that is an answer. I am asking you as the chief lawyer for Yahoo!, is an e-mail from some sheriff in some county stating "I am the law, I am doing an investigation, I have a right to this information, give it to me now," is that a requirement that you would adhere to or would you go fight it in court?

Mr. CALLAHAN. That is not something we would provide your information to, sir.

Mr. SHERMAN. Okay. What if the letter comes from the NSA instead of a sheriff?

Mr. CALLAHAN. Again, sir, you are asking for my interpretation of something that is obviously very big in the news. I can say that would only furnish information in compliance with law.

Mr. SHERMAN. Okay. And you were willing to tell me that law does not require you to give my information to a county sheriff, but you are not willing to tell me whether law would require you to give it to the NSA in the absence of a court order of any kind.

Mr. CALLAHAN. I was responding, sir, and our policy, of course, is not to respond on specific interactions with law enforcement. I will tell you that we would not furnish anyone's information unless it was in compliance with law.

Mr. SHERMAN. Okay. And I will ask all of you who operate in China, what have you done to tell your Chinese customers that they have a lower expectation of privacy and that you will comply not with the law of your democratically elected host government, namely the United States, but rather that you will furnish information upon the request of an un-elected, un-democratic and oppressive government in China?

These guys who are going to jail might die. Were they at least notified that that could happen to them?

Do we have a response from anybody who does business in China?

Mr. SCHRAGE. I actually do not know what kind of notice we give because we do not offer that possibility. We do not offer the service.

Mr. SHERMAN. I guess this is really address to Yahoo! and to Google.

Mr. SCHRAGE. I am representing Google. We do not offer the service.

Mr. SHERMAN. You do not offer an e-mail service?

Mr. SCHRAGE. Right. Where the data is maintained in China so it is not subject to Chinese law. The only way——

Mr. SHERMAN. Well, wait a minute. The Chinese could tell you that under Chinese law they are expropriating all your assets in China unless you reveal information on your server in the United States. Then what do you do? What do you tell your shareholders when you lose hundreds of millions of dollars to stand up for principle? Are your shareholders willing to do that for you?

Mr. SCHRAGE. My understanding is that the only legally appropriate way for the Chinese Government to request e-mail information that is stored on servers in the United States would be to follow a process——

Mr. SHERMAN. What if they told you that under Chinese law your United States-based employees had to give them that information and if you did not comply within 24 hours all your assets in China were gone, your right to do business in China, your stock is about to drop by 20 percent, what do you do?

Mr. SCHRAGE. I am not going to say we are going to give them the data, if that is what you want me to——

Mr. SHERMAN. Nor are you going to say that you will not give them the data.

Mr. SCHRAGE. I think, again, as with the other question, it would be a terrible situation.

Mr. SHERMAN. Could you not tell your Chinese customers albeit logging onto a United States-based site that you cannot assure the United States Congress that you are not going to rat them out if the economic pressure becomes intense?

We are talking about whether people go to the goulag or not. Should they not have a right to know whether their e-mails on your servers in the United States are safe or are not safe from the Chinese Government?

Mr. SCHRAGE. I think the likelihood of the scenario you are suggesting is really very small.

Mr. SHERMAN. You don not think the Chinese Government would use economic power in order to get information that they need to

oppress people? Or you think they are just not interested in oppressing people?

Mr. SCHRAGE. I would like to think that the Congress and the United States Government might think that that exercise of power——

Mr. SHERMAN. Okay. That is why I am going to ask you next. Would you support a U.S. law that would answer that question for you and say that no U.S.-based employee can turn information over to an oppressive government unless there is a certification from the United States Government that it is a legitimate investigation of a legitimate non-political crime?

Mr. SCHRAGE. Again, I do not know the specifics of what you are saying, but in theory we would support that kind of additional support. Sure.

Mr. SHERMAN. Yes. I cannot ask you to support a bill that has not been drafted yet, so I will be in touch with you.

Mr. SMITH OF NEW JERSEY. Will the gentleman yield?

That is precisely where our bill goes, so I am glad to hear of the support from Google.

Mr. SHERMAN. Good. We will list them as a co-sponsor. It will be the first Smith-Google bill.

Gentlemen, I have asked you some tough questions. I want to applaud you for the vast majority of the electrons in China that you are responsible for. The vast majority of Internet use in China is helping to open up that society and we have to make sure that in our effort to prod you to—should I use the phrase "not be evil" that we do not throw out the baby with the bath water.

Mr. Chairman, do I have any more time?

Mr. PAYNE. Would you yield for a moment?

Mr. SHERMAN. I will yield.

Mr. PAYNE. I just want to make it the Smith-Payne Google bill.

Thank you.

Mr. SMITH OF NEW JERSEY. Thank you, Mr. Sherman. I really appreciate it.

Mr. SHERMAN. Thank you.

Mr. SMITH OF NEW JERSEY. Let me just ask you, if you would, to take back three questions, maybe even four. I had asked this earlier and I know that, Mr. Callahan, you pointed out that you are prohibited by Chinese law to tell us and to provide for these Subcommittees how many Chinese requests, is it on a daily basis, weekly basis, on average do you receive, but if you could take back and provide us for the record, all four of you, if you would, as it relates to your companies, one, how many Chinese requests on a daily or weekly average do you receive, we will give you this in writing, to censor content, provide information about users, remove Weblogs, update or fine tune filtering equipment?

Secondly, what legal process does China use, what documents does it present, how specific are these documents or papers when they make those requests?

Number three, can you describe your established procedures for handling Chinese requests for user information, both past and present, on user information or censorship?

Are their requests for clarification automatic referral to U.S. headquarters and legal counsel?

Is there an appeal process? Do you say, "Wait a minute, we do not think that should be provided"?

And, finally, in what circumstances would you refuse a Chinese request?

And, finally before yielding to Chairman Leach for some questions that he wanted to pose, Mr. Lantos brought up the issue of discrimination against women and I do have a question I would like to ask.

For years, I have led an effort to bring focus and scrutiny to the horrific practice in China of forced abortion and coerced sterilization. It is a direct consequence of the one child per couple policy.

As a matter of fact, we have in our audience here—Dr. John Aird, the late great Dr. Aird—a widow who was married to Dr. Aird for 58 years, Laurel Aird, and we are so grateful that she came to this hearing, but Dr. Aird wrote a book and he was the senior research specialist on China for the U.S. Census Bureau, so he was the top person within our own Government that tracked what was going on in China and he wrote a book called *Slaughter of the Innocents*, heavily footnoted, and he wrote many times thereafter about this disgraceful process where women have to get permission to have a child. They are told when and if they can have the one child. Brothers and sisters, like I said in my opening comments, are illegal. It is the only place in the world where they are absolutely illegal unless the government says you can have a brother or a sister. And it has led to gendercide.

There may be as many as 100 million missing girls in China which also becomes a magnet for human trafficking, bride selling, plus the terrible crime that is committed against baby girls simply because they are baby girls and they are aborted through sex selection abortions in China with incredible tenacity on the part of China.

My question is—and let me also say, parenthetically, because we have referenced the Nazi dictatorship a number of times today, at Nuremberg, forced abortion was construed, and properly construed, to be a crime against humanity against Polish women. It is a horrific crime and it is practiced, it is commonplace in China, just like torture and other crimes that are committed by the government.

Again, discrimination against women, does your technology in any way, whether it be the censoring of e-mails, we know that women have children on the run and some of them are to evade the family planning cadres that way. I had a series of hearings and women sat right where you sit today, one woman who found an abandoned baby girl, made that girl her own like the Good Samaritan, only to have the family planning cadres knock on her door and say the one you are carrying has to be aborted and she broke down in tears. She was on the Golden Venture, as a matter of fact, and came here and was seeking asylum here and spent about 3 years in our own detention camps in Bakersfield before she was able to get free.

Having said that, does any of your technology, your e-mail as well as those who might type in trying to find some help to evade this coercive population control program, does any of your technology get to be used against those women?

I know you may not have that answer for here today, but I would ask you to take that back, having met so many women who have been coerced into abortions over these many years and having had many even sit here at witness tables, Harry Wu brought a woman out of China named Ms. Gao, and I will conclude on this, who ran a family planning program in Pujin Province. Harry Wu, of course, will be up in our next panel. She said right where you sit, "By day I was a monster, by night a wife and mother," and she talked about how octopus like this network was to discover when and if women were pregnant. They monitored their menstrual cycles. What an invasion of privacy that is. That is outrageous. And our hope is that none of your technology and none of your corporate presence as well in China is in any way aiding and abetting that. I would ask sincerely if you could get back to us with that information as well as the others, unless you wanted to comment now.

Let me go to Chairman Leach.

Mr. LEACH. Chairman Smith commented on the profoundest issue of the right of life, which is in our Declaration of Independence, but I am going to come back to the liberty issue just for a second. I realize there is a huge challenge here, the distinctions between the necessity and the good of commerce and the problem of values and I just want to ask one set of questions just to highlight it and then comment in a little different direction.

As I understand the distinction between Yahoo! and Google is that Yahoo! requires a signed statement of the government to censor something. It is my understanding you censor Voice of America and Radio Free Asia. Is that correct?

Mr. CALLAHAN. Sir, I think there were two things that we discussed. The first was with respect to information on a user that we had to furnish, in the Shi Tao case, that was mentioned. That was pursuant to a lawful order that was signed and authorized.

As to censorship, we do not have a day-to-day operation in China any more, but at the time, my understanding was there was a list of prohibited sites from the government.

Mr. LEACH. So you have a piece of paper that they request for Radio Free Europe and Voice of America?

Mr. CALLAHAN. My understanding is that they would give that out to the companies for blocking purposes, yes.

Mr. LEACH. And then with regard to Google, you would do this on your own, based upon the practices of others? Is that right?

Mr. SCHRAGE. Congressman, my understand is that——

Mr. LEACH. Would that have been in your license that you had to apply for?

Mr. SCHRAGE. What my understanding is, and, again, I have not read the license, I do not read China, my understanding is that the license requires us to comply with the law. I believe that in certain cases were given a list of URLs of sites that we have to block. My understanding is that there may be some additional stuff that we are required to do.

Mr. LEACH. But you do block Radio Free Asia and Voice of America? And presumably the BBC—would this apply to the BBC?

Mr. SCHRAGE. I do not know that. I would assume that, but I do not know.

Mr. LEACH. Well, I just raise this again, that you are both American companies and you are blocking American voices and that is an extraordinary phenomena.

Then I want to comment on a little bit the very powerful and very thoughtful statement of Mr. Wexler and his one point is absolutely valid, that it is principally the responsibility of the United States Government to do certain things. Corporations can do some thing and not do others as well, although corporations do have values, just as individuals have values and a corporation can make value judgments and often value judgments are competitive. There is a value judgment on certain censorship, there is a value judgment on whether opening to more information is a basic good. And so you have competing values on these judgments and you also have different constituencies. One of the really interesting phenomenons that this brings out very thoroughly is that there is a difference between a country and a government and a stockholder and your duties are first to your shareholders in many instances, although not all. And so these become competing values.

It also underscores that maybe your government has reason to be acting in given kinds of ways and my concern a little bit is that I think that there is value in making an issue transparent and this hearing is part of the transparency of an issue and it shows your dilemma, it shows the dilemma of the Congress.

The can be productivity in government actions and legislation. There also can be counterproductivity and we often do counterproductive things as a government; and so one of the really big questions that we are all going to have to search through is whether this is a subject that is relevant and appropriate constructively for legislation and, if it is, what that legislation might be.

Now, one of the things that has been placed on the table this week which is new to this whole issue is the decision of the Secretary of State to form up a task force and I hope it is a task force that gets a lot of input from the private sector in a constructive way, likewise, with Congress. We are going to be very careful of this particular direction we go in.

My own personal sense is that Congress would be very wise to work with the State Department's task force as we attempt to develop legislation, if that is the path we go on.

I just raise this because I think this hearing will come to an end today on the basis of transparency issues, but what unfolds afterwards is going to be something thaIs going to have to take a lot of input from a lot of different sources and I think that this group of people at the table are going to want to be very attentive to it.

I will tell you, the embarrassment that should apply to any government that censors is very large and so to a large extent that is where the principal embarrassment goes. Whether despite all the ironies that you are the symbol of expansion of knowledge in the world today companies, to cut off knowledge is obviously awkward and I think all of you recognize that. It is particularly awkward because you are not only American companies, at least one of you and possibly all of you have partial ownerships in Chinese companies that are active, if not leading, in complying with this sort of thing. And so for a company to set its own standards and then have those standards be based upon the standards of a company that it is a

part owner of is awkward as well. So you are seeing international commerce in many ways come together in a rather extraordinary set of ways and I just hope that your management thinks things through, as Congress is going to have to think it through.

We in the press sometimes what are called ombudsmen to look at what the press does and it is not inconceivable to me that corporations might think in that way as well.

Thank you very much, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. Chairman Leach, thank you so very much.

Just as we conclude and go to panel three——

Mr. SHERMAN. Mr. Chairman, if I could just ask a question or two for the record?

Mr. SMITH OF NEW JERSEY. Mr. Sherman.

Mr. SHERMAN. One of those and perhaps you could just get back to us soon is for your Chinese customers or your American customers, this is really a technical question, if they delete an e-mail, is it deleted? Or is it still in your files available for whatever judicial process proceeds?

This assumes, of course, that the other party to the e-mail obviously may have a copy of it or may have deleted it as well.

The final comment I'll make, if the Chairman will indulge me, is on the whole censorship and flow of information.

Every time I go to the arcade and I play Whack-A-Mole, the moles win because I whack one and two pop up and I would hope that his Congress and perhaps the technical talents in front of us here, that Congress would provide, whether it is to Falon Gong, whether it is to Google, whether it is to Yahoo!, whether it is to Cisco or whatever, contracts to figure out how to punch homes through these firewalls, how to make sure that the content pops up; even if it is blocked here, it comes out over there. And I am confident that with your technical backgrounds and capacities and with perhaps some congressional appropriations that every time China tries to suppress information in one way it will pop up in two other places.

I yield back.

Mr. SMITH OF NEW JERSEY. Mr. Payne?

Mr. PAYNE. Let me just thank the Chairman once again for calling the hearing and for this panel, of course, we have another panel, for your attempt to clarify some of these issues.

I hope it is clear when you get back to your associates and they get back to their board members and their stakeholders that Members of Congress are pretty serious about this issue. Your job is the messenger. We tend to slay messengers from time to time; however, we are very serious about this. We are still the United States of America, we are still the country that is supposed to set the tone and we are still the country that expects our corporate leaders and our civic leaders and our political leaders to also set a tone that separates us from the rest of the world. We certainly will not condone cooperation with people who, as you have heard from the questions here, are very serious about trying to have some impact on what happens.

Now, we have a lot of companies that do business in China, not only yours, and we have the same kind of disdain for their behav-

ior, too, because they go along to get along. On the one hand, we hear our business leaders applauding the tremendous economic leap in the PRC and how great they are doing business wise and then we have Secretary of Defense Rumsfeld come back and is grumbling about the fact that they are spending so much money on military equipment and stealth submarines and all kinds of offensive weapons that he contends may someday be used against us.

It becomes baffling sometimes to decide whether they are our great friends and we will change them or will they be our enemy. It really makes no sense. In some instances, we talk about how strong they are getting. If it were not for the U.S. and our tremendous of balance of trade deficit, they would not be in the position that they are in.

Now, I am not saying it is bad or it is good, it is something that is difficult to explain. I expect that the message that this Committee and these two Committees that we have conveyed, at least a number of us who are very serious about this, is that business as usual is really not going to be the way to go and that you need some help perhaps from the U.S. Government. We in Congress intend to give some tools to help your companies to defy or at least challenge by virtue of our law. They do not want you to violate their laws; well, we do not want you to violate ours either. And so there is going to have to be some other way to look at how we deal with this. As I indicated, we are serious about it and I am sure that we will be looking forward to the responses that Members have asked for you to send back to the Committee.

Thank you, Mr. Chairman.

Mr. SMITH OF NEW JERSEY. As I conclude, let me just thank you and I think the record should make very clear, you all came voluntarily. There were no subpoenas issued and for that both Subcommittees are very grateful.

This will be a dialogue and an exchange that will continue. We will give you a copy of the bill that I will be introducing tomorrow, Mr. Payne is our principal co-sponsor, called the Global On-Line Freedom Act of 2006. Like any other bill, it begins its uphill climb beginning tomorrow morning. We would welcome your input and your thoughts on what you think is contained in this and we would ask all of the panelists and, of course, the Administration if they would do likewise.

Thank you for being here. We appreciate your participation. Thank you. Beginning first of all with Harry Wu, who was first arrested as a young student at the Beijing Geology College for speaking out against the Soviet invasion of Hungary, and criticizing the Chinese Communist Party.

In 1960, he was sent to the Laogai, the Chinese Gulag, as a counter-revolutionary writer. He was finally released in 1979. Mr. Wu came to the United States in 1985. He was the author of *Laogai—The Chinese Gulag*, a theoretical explanation of the Laogai system in Communist China. He also wrote *Bitter Winds*, his autobiography, published in 1994; and *Troublemaker*, which was published in 1996. Mr. Wu is currently the Executive Director of the Laogai Research Foundation, and head of the China Information Center.

We will then hear Libby Liu, who was named the President of Radio Free Asia in September 2005 by the Broadcasting Board of Governors. Ms. Liu served previously as RFA's Vice President for Administration and Finance. Prior to joining Radio Free Asia, Ms. Liu served as Director of Administration and Strategic Planning at the Baltimore-based National Association for the Advancement of Colored People, or the NAACP.

We will then hear from Xiao Qiang, who is the Director of the China Internet Project at the Graduate School of Journalism, University of California at Berkeley. Mr. Qiang became a full-time human rights activist after the Tiananmen Square Massacre in 1989. Mr. Qiang was a former Executive Director of the New York-based NGO Human Rights in China. He was the recipient of the MacArthur Fellowship in 2001, and profiled in the book, *Sole Purpose, 40 People Who Are Changing the World for the Better*.

I note parenthetically that Mr. Qiang was at our hearing on December 18, 1996, and he had pointed out at the time that right after Tiananmen Square, that 2 days later he was on the Square doing fact-finding and gathering crucial information about what had really happened. He provided expert testimony at the hearing when Cao Gangchuan, the then-Defense Minister of China, said no one died at Tiananmen Square.

We will then hear from Lucie Morillon, who joined the French National Consultative Commission of the Human Rights in Paris in 1999. In 2000, Ms. Morillon joined the International Press Freedom Organization, Reporters Without Borders, as an assistant researcher for the European Informer, USSR desk, at a time when Meloshiv Serbia was cracking down on journalists.

She transferred to Washington, DC, in 2004. She opened a representative office in the American Capital, where she supervises Reporters Without Borders USA, in partnership with the New York City office.

Finally, we have Sharon Hom, who is the Executive Director of Human Rights in China, and Professor of Law at the City University of New York, School of Law. Professor Hom was a Fulbright Scholar in China, and served on the U.S. China Committee of Legal Education Exchange with China.

Her books include co-authored inter-disciplinary text and workbook, *Contracting Law*, co-edited *English-Chinese Lexicon of Women Law*; and an edited volume, *Chinese Women Traversing Diaspora: Memoirs, Essays, and Poetry*.

If you all would not mind standing in order to take the oath, and if you would raise your right hand.

[Witnesses sworn.]

Mr. SMITH OF NEW JERSEY. Let the record show that each of our witnesses answered in the affirmative. Mr. Wu, if you would proceed.

TESTIMONY OF MR. HARRY WU, PUBLISHER, CHINA INFORMATION CENTER

Mr. WU. Thank you, Chairman, I think this is a very important, significant hearing on China issues today. I think it is common knowledge that the people of China are still living under a Com-

munist Totalitarian Regime. I do not believe there is anyone who can honestly object to this statement.

So all these hearings, arguments, or statements have to be based on this issue. The issue that, until this moment, this is a Communist Totalitarian Regime.

As technology has developed and expanded, the Chinese community has correspondingly developed and expanded its knowledge and its abilities to control it. So when we are talking about these 100 million people on the Internet, we have to be aware that there are 35,000 so-called Internet police right now, working in the public security ministry. Their job is to control and monitor who are on the Web sites and in the chat rooms.

By the way, Chairman, can I submit my written statement?

Mr. SMITH OF NEW JERSEY. Without objection, your written statement, as well as the written statements of all of our witnesses and any attachments you would like to provide for the record will be made a part of the record.

Mr. WU. Because a lot of witnesses are going to be talking about censorship, and the Chinese dissidents who were captured by Chinese security. I just want to briefly go through my Power Point.

This is a police notice. It is very common everywhere in Chinese cafeterias. The notice says that all Internet users must register and use a Government-issued ID. If they do not have an ID, where do they go?

All this computer access in the cafeterias, they have received software from the local Government. That means the local government can right away, for security, find out who you are and what kind of Web site you are visiting. It is by law.

I think these four companies over here just testified that they knew about this. Then there is a number of people who do research, these so-called cyber-dissidents. This shows one sentence, 5 years in prison in 2003; and the other is cyber-dissident Du Daobin, who was sentenced to 4 years, just because of an article posted on a Web site. Shi Tao, I think everybody knows about that. Another one is Li Zhi, who got 2 years in jail.

So I think this kind of situation, these people, these companies, have a great deal of business in China. They are aware, but they just try to tell different stories. They say, our technology is helping the Chinese to improve communication. So that means we are helping people to fight for democracy and freedom.

We know that technology can be used by every side. It is not only used for democracy. It is also used by the government to control.

Let me focus on one thing. Because most Americans in China are working for a legitimate company or institution. It is not too late to point out that Cisco is directly working for Chinese security.

For example, we have this brochure, this Chinese-language brochure from Beijing University. Chinese Leader Jiang Zemin was there. Prime Minister Zhu Rongji was there, and this university, this institution focused on one program, and this program was Chinese security talking about fingerprints.

So here, on page 11, PKU (Peking University), the police were right here. This said, MIS, for criminal investigation, large-scale fingerprint scanner; MIS for Social Security fingerprint verification system for access control and personal identification system for na-

tional security. China President Jiang Zemin, Prime Minister Zhu Rongji, and many other state officials visited the company and gave the product high praise. Many world-famous industry leaders, including Intel, Sun Microsystem, Cisco, Compact, HP, have built cooperative relations with this company. Beijing University, our company is there.

Now let me focus on this other issue. Because this is a kind of product that has a dual purpose. Unfortunately, Cisco—let me show you this brochure. This brochure was obtained in 2002 in Shanghai. There was an exhibition, and there were many companies. Most were American companies that were involved. Of course, Cisco was there.

I will show this. I have obtained this in the Chinese language. So you can see the first page, and on the second page, you can see that Cisco said, "We can help you make your work more effective." The next one, it said, "Enhancing the police force." Then, in the other one, Cisco gives you a case that in Qinghai Province, they already set up a kind of network for public security.

Then I will give you another case from Yunnah Province. There was public security by Cisco to set up a whole province-wide surveillance system. I just listened to the gentlemen right here, just a couple of minutes ago. He said, well, we are doing something. For example, we helped the ambulance connect with the students. They are connected with the stations. Actually, it is right, but the words you used were wrong. It was not an ambulance. It was patrol car. Here is another photo you can see, a patrol car.

They helped the police in that province, from patrol car to patrol car, patrol car to the station, police station, to effectively work out.

Congressman Smith, you know that I always want to go back to China. But right now, I am very scared, because they have very effective systems to find out where I have been.

This fear is not only, today, in China. It has come over here. You just heard Mr. Li was beaten by someone here because he is the chief technician of the Yahoo!, of the Falun Gong. I think this is a very serious message given by the Chinese and given to the people over here. Terry Alberstein, Director of the Corporate Affairs of Cisco Systems, Asia Pacific, maintains that Cisco, just like today the representative here says, Cisco sells networking equipment to law enforcement agencies around the world. They insist that their business activities in China are therefore identical to those in other countries.

However, Terry said, we are specifically talking about China. There is no specific United States law that prohibits the export of crime control equipment to China.

But here is the law. This law forbids Americans from exporting any equipment for crime control or detection; not for other countries, just for China. If Cisco convinces people by saying in their statement that Cisco does, however, comply with all American Government regulations, which prohibit the sale of our products to certain destinations or to certain users or to those who re-sell to prohibited users. We have not sold and do not sell our equipment to the countries listed on the U.S. Department of Treasury or SEC list of embargo nations; and we comply fully with all aspects of the

Foreign Relations Authorization Act as passed by the Congress in the wake of the Tiananmen Square incident.

If Cisco tries to convince you, or convince the media, that they are not cooperating with Chinese security authorities, why not just tell the people what is your contract. I made my own investigation. These contracts are not only in Yunah or in Qinghai Province—even this Chinese report said that Cisco made an announcement in 2004 that they helped the Public Security Ministry to improve their Golden Shield Project. The Vice President, Jiang Shihua, of Cisco management, the Vice President in China said, we are very happy to work together with the Chinese public security in improving the Golden Shield program.

In China, in the public security system, the number one VOIP system, according to Chinese news, was established by Cisco.

Also, this program, this contract from Cisco, included training. We want to ask Cisco, who are these people in your training program. So far, we learned that all of them are Chinese police. It is not only offering the technology and software devices, but also training.

If Cisco can publicly tell the people, saying we have one, two, maybe five, maybe ten contracts with the provincial security systems, and so far as I know, it is millions of dollars. One of them is $8 million in 3 years. Then they can convince the people by saying they are innocent; they do not work for the Chinese security and do not violate American law. Thank you.

By the way, there is a money manager group called Boston Common. Year after year, they intend to fight against the Cisco management. Because Boston Common represents 22 billion customers, and they disagree with Cisco's decision to work for Chinese security. I hope we can put Boston Common's statement as a reference in the *Congressional Record*, thank you.

[The prepared statement of Mr. Wu follows:)

PREPARED STATEMENT OF MR. HARRY WU, PUBLISHER, CHINA INFORMATION CENTER

First, I would like to thank Congressman Henry Hyde and Congressman Chris Smith for convening this hearing today on the important issue of Internet suppression in China. Thank you for your consistent support of the rights of the Chinese people and the work of organizations pushing for human rights in China.

In President Bush's speech in Kyoto during his recent trip to Asia, he urged China to take steps to promote freedom and democracy. What poses a challenge to freedom and democracy in China is not only the Beijing government, but also international companies that provide financial and technological assistance to the Beijing regime, allowing it to maintain its control.

It is common knowledge that a communist regime such as China's maintains total control over all forms of media—television, radio, newspaper and the Internet. The Chinese Communist Party has its own Propaganda Department, which ensures that all media content is consistent with official political doctrine. As technology has developed and expanded, the Chinese government has correspondingly developed and expanded its knowledge and its abilities to control it. As an example of this, there are currently at least 35,000 so-called "Internet police" in the Public Security Ministry whose job it is to monitor and censor websites and chatrooms in China.

From diplomacy and trade to strategic alliances and multilateral treaties, the last decade saw increased interaction and cooperation between the West and China. The outlook for liberalization was promising, despite China's notorious record of human rights abuses. Many argued that this type of "engagement" would lead the Chinese to a more liberal, democratic society. Others speculated that totalitarian regimes would only choke the liberating powers of the Internet. Unfortunately, current evidence suggests the pessimists are right. Censorship of the Internet is increasing

with the explicit help of high-tech multilateral corporations. Beijing is seizing this opportunity to squash dissent and spy on its population with unparalleled efficiency.

While the introduction of technology into a society can be a positive force for change, it is important to consider the fact that technology can be used by all sides, and can therefore also be used as a negative force. In the current debate over the actions of American IT companies in China, these companies have asserted that they have provided the same technology and equipment that they have provided to all other countries they do business with. They maintain that they are not responsible for the ways in which their customers use the technology that they sell, and that they do not alter it in any ways to serve the needs of a particular customer, such as China's communist regime. They also argue that they are providing a positive service for the Chinese people by giving them technology and enabling them to have access to the outside world. But we must remember that this technology is like a pistol that can be used by all sides. While it can be used by the Chinese people, it can just as easily be used by the Chinese government to oppress them.

Information technology is often heralded as a tool to promote democracy, because it allows increased transparency and the liberalization of communication. But those living under authoritarian regimes cannot communicate with the world, or each other, freely—their right to privacy and free speech does not exist. China currently censors foreign and local media, and also suppresses dissent, but how far will China go in the name of "social stability"? Sadly, China is undertaking a monumental effort to monitor and track its citizens.

A friend of mine recently tried to access some politically sensitive websites while at an Internet café in a remote, small city in Xinjiang Province. The police quickly showed up to arrest him. I don't know who supplied the technology enabling the police to track my friend's Internet surfing, but I am pretty sure that U.S. technology was involved. The PRC's Ministry of Public Security has been continually upgrading and expanding its $800 million "Golden Shield" project—a government-sponsored surveillance system that was begun in 1998. The Golden Shield's advanced communication network was supposedly aimed at improving police effectiveness and efficiency. However, China has also used the "Golden Shield" as a way of monitoring Chinese civilians. The project will help prolong Communist rule by denying China's people the right to information. In order to develop the "Golden Shield," China has utilized the technologies of a number of foreign companies, such as Intel, Yahoo, Nortel, Cisco Systems, Motorola, and Sun Microsystems. The "Golden Shield Project" would not have been possible without the technology and equipment from these companies.

China has recently been clamping down hard on Internet cafés. Currently, everyone who wants to access the Internet at Internet cafés throughout China must register with their real names and present their identification card each time they come to surf the Net. This effectively prevents Internet users from even attempting to access any websites that the Chinese government deems inappropriate or politically sensitive. Government authorities throughout China have installed software in the computers in Internet cafés, enabling them to carry out comprehensive, long-term monitoring. This technological control software is capable of obtaining real-time information about Internet users, and can also keep a record of instances in which Internet users exceed the Internet curfew.

While technology can be used to improve communications systems, it is clear that it can also be used for suppressive purposes. Today, the American IT companies that are present in China are working together with a totalitarian regime, that of the Chinese government. Therefore, despite the publicly-stated goals of these companies to provide Chinese people with greater information and access to the outside world, it is difficult for them to avoid working together with the immoral, corrupt Chinese regime.

Recently, there have been a number of cases in which Chinese "cyber-dissidents" have been sentenced to years in prison or placed under house arrest simply for sending e-mails or expressing their views online. China currently has the largest number of jailed Internet dissidents of any country in the world. From the following slides, we can learn about the cases of cyber-dissidents Huang Qi, Du Daobin, Shi Tao, and Liu Shui:

- On May 9, 2003, Huang Qi, founder and editor of the Tianwang website, was sentenced to five years' imprisonment for "subversion".
- Cyber-dissident Du Daobin was sentenced to four years of house arrest on June 11, 2004.
- In April 2005, journalist Shi Tao was sentenced to 10 years in prison for "divulging state secrets abroad".

- Cyber-dissident Liu Shui completed the two-year sentence of reeducation through labor which he received in 2004.

We now know that Yahoo complied with Chinese authorities in two separate incidents that resulted in the imprisonment of people for their activities on the Internet. Last week, it was reported that Yahoo released data that led to the arrest of Li Zhi, an online writer who was sentenced to eight years in prison in 2003, after posting comments that criticized official corruption. This case is parallel to that of Shi Tao, who was sentenced to 10 years in prison.

Moral responsibility for Yahoo's collaboration in the imprisonment of Li and Shi cannot be shrugged off with a simple assertion that Yahoo had no choice but to cooperate with Chinese authorities. A Yahoo spokeswoman insisted that in its dealings with China, the company "only responded with what we were legally compelled to provide, and nothing more". She argued that the company did not know how Chinese authorities would use the information it provided. However, we must ask who is making the laws and regulations requiring Yahoo to give up information about its customers. We must ask what kind of a government they are dealing with, and who they are providing a "pistol" to. The answer is that their major business partner is the Chinese government.

I would like to mention another example, involving the Beijing PKU High-Tech Fingerprint Co., Ltd., which collaborated with Intel Co. to greatly improve the speed of system operations, breaking through the limit of 100,000 prints per second. The capacity of the fingerprint database that was created exceeds 5,000,000. This fingerprint identification system is a part of the Public Security Bureau's (PSB) "Golden Shield Project", and is just one example of how the project is used to monitor and control Chinese citizens.

Similarly, Cisco Systems cannot dismiss criticism of its "Big Brother" censorship activities in China by maintaining that China's use of its equipment is beyond its control. Cisco Systems recently publicly confirmed that it has done business with China's PSB, and that it also provides service and training to its customers, who in this case they know are police officials. Cisco Systems, unlike other IT companies, has signed contracts *directly* with Chinese public security authorities.

Terry Alberstein, Director of Corporate Affairs for Cisco Systems—Asia Pacific, confirmed that Cisco does indeed sell networking and telecommunications equipment directly to Public Security and other law enforcement offices throughout China. According to Rconversation.com, the website of Rebecca MacKinnon, Alberstein said that Cisco sells to police around the world, and that it is not illegal for Cisco to do business with the Chinese police, because the equipment sold is not prohibited under the Foreign Relations Authorization Act. Mr. Alberstein reiterated that Cisco is doing nothing against U.S. law, and emphasized that Cisco does not tailor routers for the Chinese market and does not customize them for purposes of political censorship. According to Alberstein, "The products that Cisco sells in China are the same products we sell in the U.S. We do not custom-tailor any product for any export market." Also, an e-mail from Cisco Systems' public relations department that was also posted on Rconversation.com states that "Cisco Systems does not participate in the censorship of information by governments."

I'm glad Cisco has publicly confirmed that it has done business with China's Public Security Bureau, and that it also provides service and training to its customers. While Mr. Alberstein asserts that Cisco has not violated American law through its business dealings with the Chinese police, this is not up to Mr. Alberstein to decide. The U.S. Congress has the authority to decide if any violations have been committed. Cisco's technology and equipment have without question made the job of Chinese police easier and more effective. Cisco has assisted Chinese security forces with their monitoring capabilities, and Mr. Alberstein lacks the authority to say that this does not constitute crime control, which would be in violation of U.S. law.

Mr. Alberstein maintains that Cisco "sells networking equipment to law enforcement agencies around the world" and infers that its business activities in China are therefore identical to those in other countries. However, we are specifically talking about China, and there is a specific U.S. law that prohibits the export of crime control equipment to China. We should not believe the argument that Cisco's sales of high-tech equipment to China are as innocuous as such sales to some other countries, and we must remember that there is a country-specific law in the Tiananmen Sanctions contained in Section 902(a)(4) of the Foreign Relations Authorization Act for Fiscal Year 1990–1991 (Public Law 101–246).

We should now ask Cisco to make public the information about exactly how much business it has done with China's PSB. Every Cisco shareholder has a right to know about this information. Cisco should publicize its profits, the quantity and date of its sales and business dealings, and its contacts in China, as well as the specific

types of software and technology that have been sold. After Cisco has truthfully revealed this information, Congress and the American people can decide whether or not Cisco has committed a violation of the law.

Unfortunately, Cisco's sales pitch has been quite successful. Through several telephone inquiries to local managers of Cisco Systems in China, it was confirmed that nearly all of China has been employing Cisco's surveillance technology in provincial, district and county police agencies. Anyone departing from the Party line is considered a threat to "social stability." Cisco Systems' technology guarantees speech recognition, automated surveillance of telephone conversations, integration of biometric data, wireless Internet access to track individual users, video surveillance data from remote cameras back to a centralized surveillance point, etc. Indeed, the prospect of China's Golden Shield is unsettling for those for have worked so hard for a democratic China.

American law prohibits the export of devices that are to be used for "crime control", but perhaps we need to reevaluate the definition of a "crime control" device. Should this law apply only to metal handcuffs, or might it also apply to electronic handcuffs? Chinese citizens who were jailed for simply expressing their views online or for sending e-mails might have a different view about this definition. Manufacturers of handcuffs aren't allowed to sell their products to China's police, but Cisco and other companies are selling the Chinese authorities much more useful technology. U.S. export laws also ban the export of dual-use technology, and we may need to look at how "dual-use" is interpreted. When companies work together with the public security authorities of an oppressive regime, should we be concerned that the technology being provided will be used toward an evil purpose, and not just for its original purpose? I believe we should.

Selling advanced technology to China not only has strategic implications, it also prevents dissent and discussion that would otherwise play a positive role in reforming China's autocratic government. The U.S. spends millions of dollars to spread democracy. Why are we allowing American IT companies to undermine our message? Continued sales of high-tech equipment will strengthen China's ability to suppress democratic voices, and further tighten its grip over the Chinese population.

Cisco

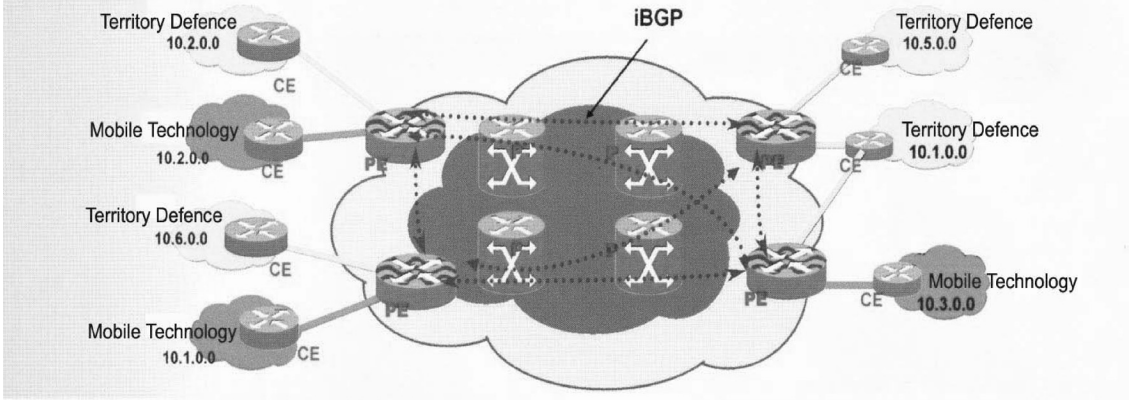
June 19th, 2003

Cisco's Sales Pitch

- Insufficient Police Force
- Unaccountable Migrant Labor Population
- High Tech Criminals
- WTO's Challenge to Battle


Video Monitoring-Controlling Solution for Preventive Control of Social Security
IP Telephone Solution for Police Routine Community Surveillance
Executive Mobile Solution for Traffic, Patrol and Criminal Case Police
Solution of Electronic Learning
Cisco Systems

Enhancing a Police Force: Solutions in Science and Technology



Applied Use:

Vertical Police Networks
(Individual departments dealing with secret/confidential business, phonetics, video frequency)

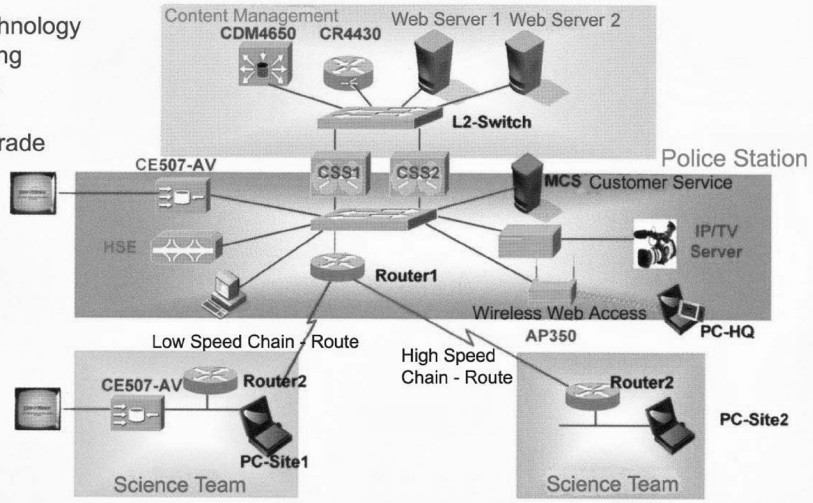
Judicial Networks
(Police, Procuratorial Courts, Supreme Court, etc)

Security, each with its own effective isolation mechanism, susceptible to expandability, compatibility, protecting investments are all priorities to central control

Working Towards Quality and Discipline :

Solutions from Computer Science

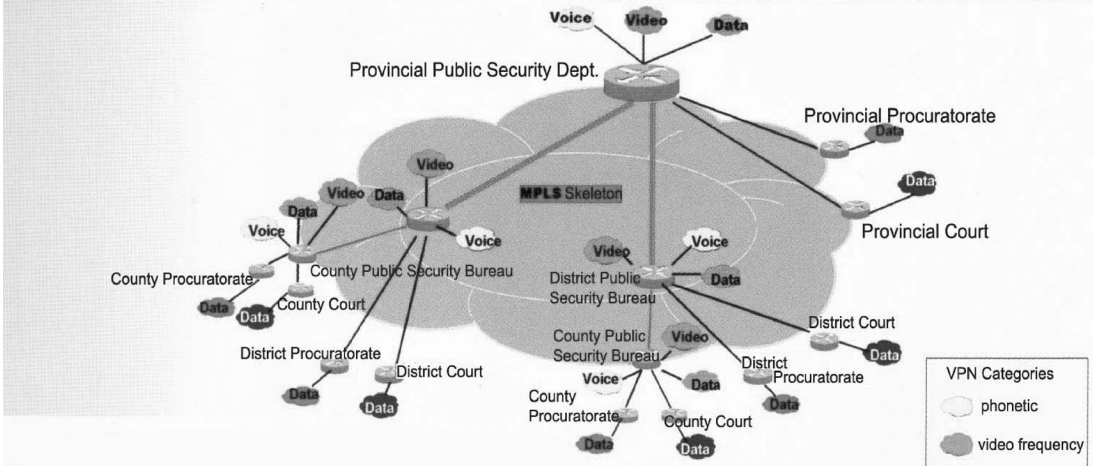
Cisco's computing technology is affordable by applying low profit margins with perfected usability for enhancing the police trade



learn law
learn police procedures
learn calculation techniques
learn etiquette
learn foreign languages

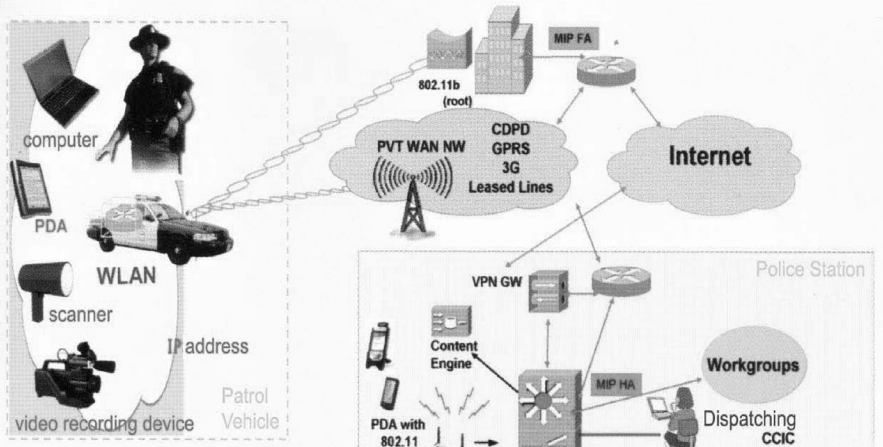
Case Study

MPLS VPN: Qinghai's Network and Navigation



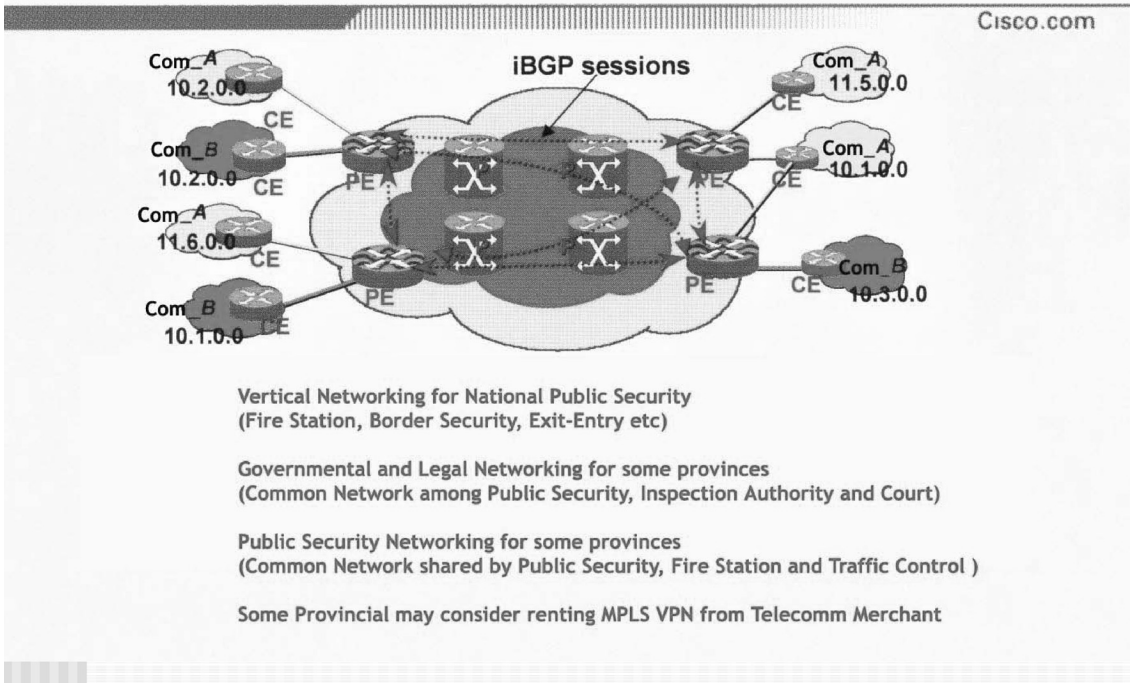
Let public security anchor and connect the courts with the special task forces. Combining phonetic, video frequency and data into one accessible resource to strengthen the country's law and order

Strengthening Communication: Mobile Solutions



Based on strategic networking when one route is busy, the network can duplicate alternate route from location

sMPLS VPN

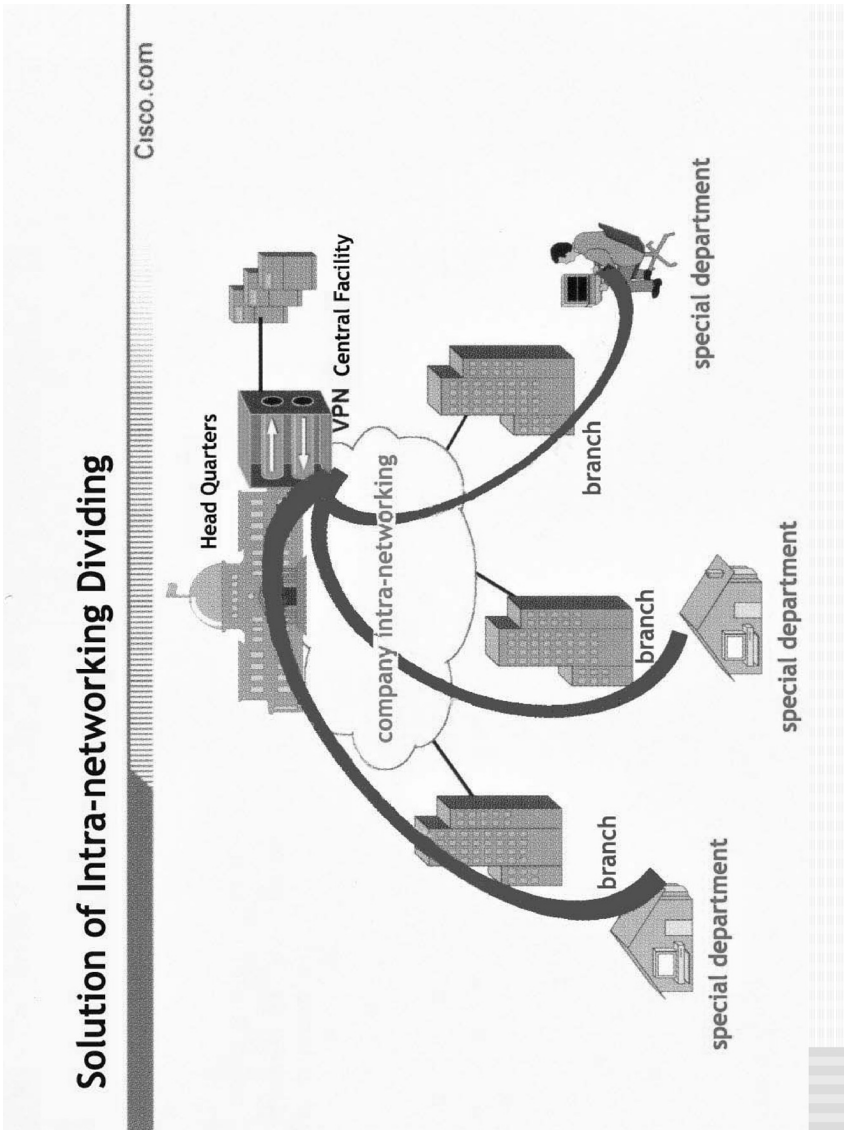


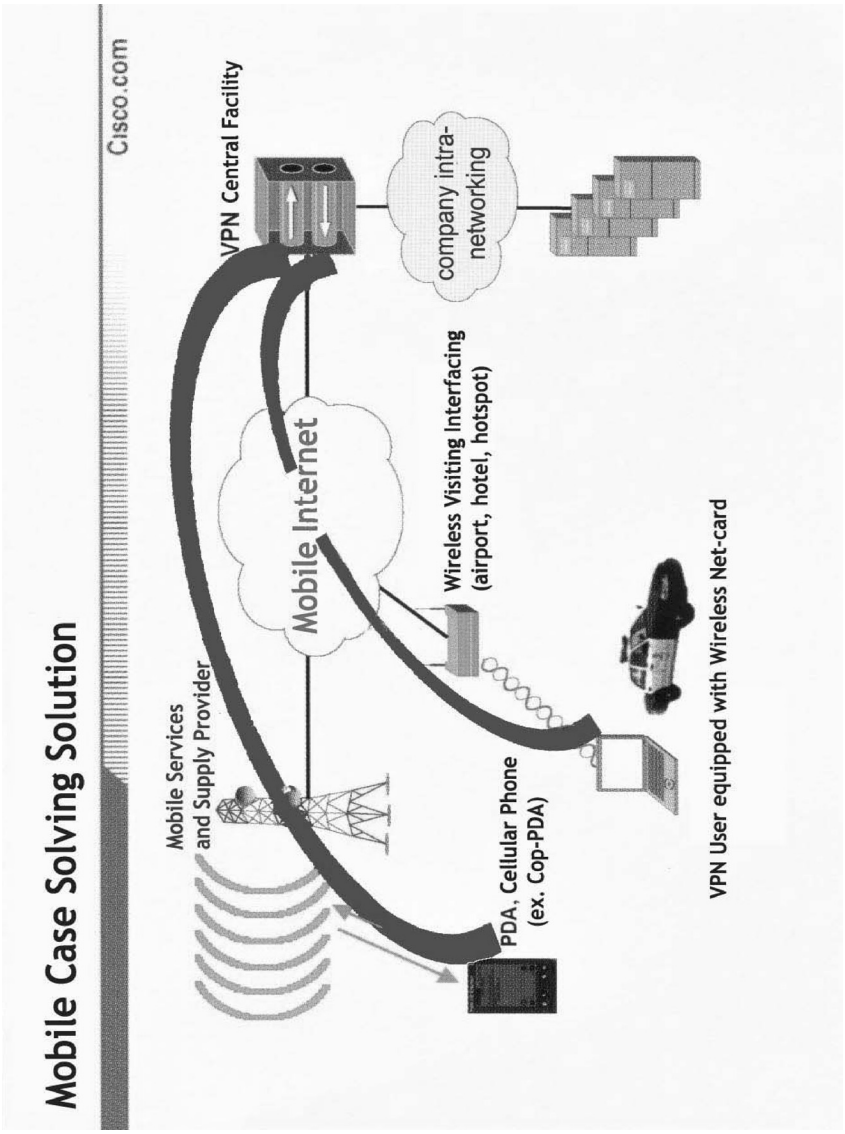
Vertical Networking for National Public Security
(Fire Station, Border Security, Exit-Entry etc)

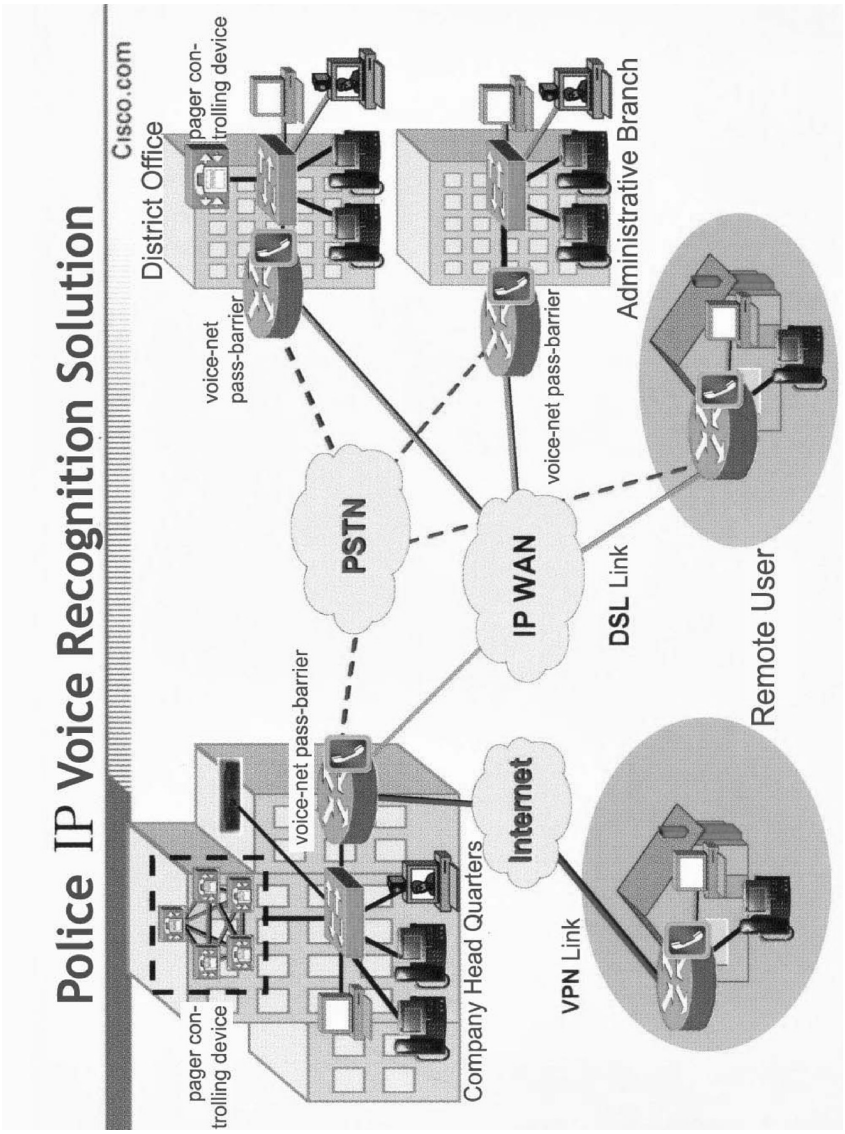
Governmental and Legal Networking for some provinces
(Common Network among Public Security, Inspection Authority and Court)

Public Security Networking for some provinces
(Common Network shared by Public Security, Fire Station and Traffic Control)

Some Provincial may consider renting MPLS VPN from Telecomm Merchant


Solution of Intra-networking Dividing
Cisco.com
Head Quarters
VPN Central Facility
company intra-networking
branch
special department
branch
special department
branch
special department


Mobile Case Solving Solution
Cisco.com
Mobile Services
and Supply Provider
Mobile Internet
VPN Central Facility
company intra-
networking
Wireless Visiting Interfacing
(airport, hotel, hotspot)
PDA, Cellular Phone
(ex. Cop-PDA)
VPN User equipped with Wireless Net-card


Police IP Voice Recognition Solution
Cisco.com
District Office
pager con-trolling device
voice-net pass-barrier
PSTN
IP WAN
voice-net pass-barrier
Administrative Branch
DSL Link
Remote User
pager con-trolling device
voice-net pass-barrier
Company Head Quarters
Internet
VPN Link

Cisco's Accountability

- Product Distribution
- Mobile Service and Supply Provider
- Technical Support through Science Team

Mr. SMITH OF NEW JERSEY. Thank you, without objection it is so ordered.

Ms. Liu.

TESTIMONY OF MS. LIBBY LIU, PRESIDENT, RADIO FREE ASIA

Ms. LIU. I would like to thank the Subcommittees for inviting me here to testify today on China's Internet censorship, and RFA's experiences in trying to get news to the Chinese people via the Internet.

I would like to take this opportunity to brief you on how Radio Free Asia is fulfilling its congressionally mandated mission to act as a surrogate for indigenous media in China, and how we have been aggressively developing new ways to expand our audience in China in the Internet age.

The good news is, our news reaches people throughout China, and is picked up by every major media outlet all over the world, hundreds of times a year. But if you try to access RFA's Web sites in China, you will most often get a message that says, "Page Not Found."

If you search the word "Uyghur" on Google.com from within China, you will be taken not only to the official Chinese site, but to a site in the Uyghur language that explains the wonders of conversion from Islam.

If you type "RFA" in the search field of Google.CN, you will get a single result. It is a link to a request for application for the NIH Web site. Bill Shaw of Dina Web told me yesterday that RFA is censored in at least three ways. RFA.org is blocked. RFA's name is blocked, and all of our content is censored.

RFA has aggressively covered Chinese cyber censorship and its aftershocks. We break and cover closures of online forums, discussion sites, Web sites and blogs. We break and cover a lot of news the Chinese Government censors out, including most recently the details of the Dongzhou Village shooting and the Taishi Village anti-corruption demonstration, despite an attempted Chinese media blackout.

These stories and many others reported by RFA demonstrate that despite dramatic improvements in their economy the Chinese people pay a heavy price for exchanging ideas. China is the world's leading jailer of journalists and cyber dissidents. Despite the fact that city dwellers can now eat pizza from Pizza Hut and lattes from Starbucks, China remains what Nathan Sharansky called a "fear society."

Radio Free Asia ensures a free flow of information into this free society, so the people of China can learn what is happening in their own country, including what their government does not want them to know.

RFA's Mandarin, Cantonese, Uyghur, and Tibetan Web sites have a unique connection to the people who live under Chinese censorship. As you know, when Chinese readers go online, they do so under surveillance and often at great risk to themselves and their families. Rarely do they get a full picture. Many sites are blacked out, whether the users know it or not. The pages they visit are recorded, the contents filtered, and their browsing patterns scrutinized. The situation is not about to improve. China continues to in-

vest in the most advanced technologies for blocking unwanted material.

The scope of China's Internet surveillance is daunting. Tens of thousands of Web police are patrolling cyberspace. Beijing has devoted enormous resources directed toward Internet and radio censorship.

Conventional wisdom has long held that the open nature of the World Wide Web and its free access to information would bring democracy to China. Today, that view looks optimistic. The question is not whether the Internet is going to change China; but rather, how much we are going to allow China to change the Internet?

As a news organization, Radio Free Asia operates in a highly unusual environment. Radio Free Asia must not only distribute that hard-to-get Chinese news, but we must teach our readers how to outsmart Chinese censors. We know we are catering to people who may not be able to read the pages, or read the pages using proxy servers, or encrypted transmissions. So our radio broadcasts have to teach our target audiences how to do that. It is a constant game of cat and mouse, and the one cost is the fear of getting caught.

On the Web, we offer live streaming of our broadcast shows. With the help of the BBG engineering, we are constantly looking for ways to evade Chinese censors and staying at the cutting edge of technology.

In October, we started offering our programs via Podcast, to multiply the number of distribution channels to make our content portable. We saw our hits spike after the Podcast was introduced.

To reach our audiences, RFA partners with a courageous and growing online community of technical experts inside and outside China. They help us get our newsletters out to the people who need them. With their help, we have created a giant network of human proxies. This network is so informal that it has no shape. But it is very much alive.

Message boards, e-mail, blogs, and instant messages pick up where the government has blocked us. Friends and family in third countries post our articles on their own Web sites, and they pass on those Web addresses.

RFA news travels fast and well by faxes, letters, phone, and word of mouth. We know that when it matters most, our news gets to where it needs to go.

What we are now witnessing is a profound change in China. That change is occurring not only in the economic and technological sectors, but, even more importantly, in the psychology of the Chinese people.

Thanks in part to the Internet, a growing number of socially aware Chinese have become loyal listeners of foreign broadcasters. Through bringing news and information to the Chinese people that they cannot otherwise access, RFA aims to promote Internet freedom by impressing on the audience that human rights include digital rights and that the freedom of expression is in real time.

In the actual townhall or on a virtual town square it is a fundamental right as enshrined in Article 19 of the Universal Declaration of Human Rights.

In conclusion, I would like to reiterate that Radio Free Asia is ably fulfilling its mission, providing journalism of the highest

standard to Asian populations whose governments aim to restrict their access to full, balanced and objective news.

RFA further is taking maximum advantage of Web technology to deliver our reporting in every available means. We use RSS feeds. We use podcasting. We welcome any improvements in the censorship situation that this Committee can offer.

Every day is a new race for technological advantages, with speeds too fast to handicap. But we have had some notable triumphs.

Nearly a year ago, thanks in part to pressure from this Congress and this Committee, Uyghur activist, Rebiya Kadeer, was released from jail and exiled from China. On May 17, 2005, she was reunited with her husband here in the United States.

RFA recorded that moment in words and photos, which we quickly posted on our Uyghur- and English-language Web sites. Barely 24 hours later, the children she left behind had seen RFA's coverage and immediately called their brothers and sisters in the U.S. to say, "We saw our parents kiss."

In a Chinese autonomous region with stringent Internet controls, the simple digital photo of Rebiya Kadeer and her husband, locked in an embrace, published online from half a world away, was a triumph.

Thank you for your attention. I would be happy to answer any questions you might have.

[The prepared statement of Ms. Liu follows:]

PREPARED STATEMENT OF MS. LIBBY LIU, PRESIDENT, RADIO FREE ASIA

Mr. Chairman, thank you for inviting me to testify today on the important topic of China's Internet censorship. I would like to take this opportunity to brief you on how Radio Free Asia is fulfilling its congressionally-mandated mission to act as a surrogate for indigenous free media in China, how it has been aggressively developing new ways to expand its audience in China in this Internet age, and why its mission today is, if anything, even more important than when our station began broadcasting a decade ago.

Radio Free Asia first went on the air in September 1996. Since then the Internet has witnessed explosive growth in China, claiming more than 110 million users by official Chinese numbers. Radio Free Asia has, in the short span of 10 years, established itself as an objective source of information for the people of China, many of whom rely upon us daily for news of the latest events and trends in their own country.

Radio Free Asia has earned the trust of its Chinese listeners and has established a reputation for being a credible source and effective disseminator of information. When domestic Chinese media fail to inform, Radio Free Asia is there to fill in the gap. In the words of a Sichuan listener who telephoned RFA Mandarin service's "Listener Hotline": "Radio Free Asia is a beacon of hope for the Chinese people." This has become particularly vital in spreading lightning-fast news concerning cyber-activism and cyber-censorship.

I. RFA is Aggressively Covering the News of Cyber-Censorship

Radio Free Asia's recent coverage of Chinese cyber-censorship and its aftershocks includes the following:

1. In September 2005, Radio Free Asia was first to report the closure of the Yannan Forum, an online discussion site that had reported the controversy over a recall campaign by villagers in Taishi in Guangdong province of their elected village chief. Before the Web closing, Yannan received a warning from the government that no news about Taishi was to be posted on this site. News about Taishi was referred to as "harmful information."
2. In October 2005, RFA reported that two Web sites, Ehoron and Monhgal, in Inner Mongolia, were closed. These sites served primarily as a discussion platform for Mongolian students. When the site managers promised not to

post any information on Mongolian separatism on the site, they were allowed to reopen in December 2005.

3. Beginning in June 2005 and continuing throughout January 2006, RFA has been reporting on the highly popular Yulun Net Web site and its blogs' periodic closures. The Web master, Lee Xinde, told RFA that the most recently closed blog, Dahe, had more than 100,000 page views since September and was the first to report on the alleged bribery of the vice mayor of Jining in Shanxi province. He also told RFA that he is instructed to close down specific blogs by the authorities.
4. On December 6, 2005, Radio Free Asia was first to report the news that protesters were being shot by paramilitary police in Dongzhou village, near the city of Shanwei, in Guangdong province. Villagers there had been protesting the construction of a power plant on land that had been expropriated by local officials. According to witnesses interviewed by Radio Free Asia, more than a dozen villagers were killed, though the Chinese government to this day insists that only three persons died as a result of the crackdown. Radio Free Asia was able to break the news of these shootings because an eyewitness had called one of our bureaus, desperately asking for help. His exact words were: "Please tell the world what they are doing to us!" Despite a Chinese state media blackout of these events, RFA.org was able to provide continuous coverage and reach its audience through small proxy Web servers.
5. Also in December 2005, RFA.org published a video account of events in Taishi village in southern China, where villagers had been petitioning since July for the recall of their elected village chief over charges of corruption. Within days, a man turned up in a local café providing vivid details of the footage. "How did you get to see that video?" asked one of the patrons. "I access the RFA Web site via proxy servers," the man answered. He invited a group to his home where, behind closed doors, they all gathered in front of his computer screen to watch the video. On that day, many people in China battling government oppression knew they were not alone
6. On January 2, 2006, RFA reported that Shenzhen in Guangdong province was the first city to use a new Web police warning system in China. When Web users log onto the Internet in Shenzhen and visit certain discussion forums, they see a pop-up figure of two police officers. This figure leads to a warning page that instructs Internet users to comply with the law. RFA reported that users felt intimidated by the pop-up and feared that it acted as a surveillance tool.
7. And just a few weeks ago, on January 24th, Radio Free Asia was first to confirm the government's suspension of *Bing Dian* ("Freezing Point"), a popular and influential weekly supplement to *China Youth Daily*. In our interview, Li Datong, the supplement's chief editor, told us that simultaneously with the paper's closure, he was notified that his personal blog had been removed from a popular Web site, on orders "from higher-up." Radio Free Asia's initial report on this crackdown on political expression was soon picked up by more than 30 major media outlets worldwide.

These stories, and many others reported by RFA, demonstrate that despite dramatic improvements in their economy, the Chinese people often pay a heavy price for exchanging ideas. According to Reporters without Borders, China is the world's leading jailer of journalists and cyber-dissidents. Despite the fact that its city dwellers can now sample pizza from Pizza Hut and savor lattes from Starbucks, China remains what former Soviet dissident Natan Sharansky has called a "fear society." As Sharansky explains in *The Case for Democracy*, "If a person can walk into the middle of the town square and express his or her views without fear of arrest, imprisonment, or physical harm, then that person is living in a free society, not a fear society. If a person cannot do so, that person is living in a fear society." By Sharansky's standard, or by any reasonable standard, China today is a "fear society."

Radio Free Asia has helped ensure a free flow of information into this "fear society" so that its people can learn what is happening in their country—including, importantly, what it is that their government does not want them to know.

Beyond the benefits to the Chinese people of having a source of objective news and a forum for communicating freely with one another, the potential benefits to the United States are considerable as well. The Rising China—both economic and military—has brought home to us the importance of providing this closed society accurate, unbiased news and information beyond what its leaders allows its people to have.

Authoritarian governments are heavy handed in controlling access to information. More complete information, and greater exposure to competing political viewpoints, help ensure that populations in closed societies are more likely to approach the outside world, including the United States, with an open mind.

Even where citizens of foreign countries are managing to obtain greater access to news from third parties, these sources are far from being substitutes for the work of entities such as Radio Free Asia. On this point, the Chinese government certainly seems to agree. Why else are they so aggressively trying to block access by the Chinese people to our Web site? And why do they devote so much effort and money to jamming our radio broadcasts?

II. RFA is Aggressively Expanding Its Audience in the Age of the Internet

RFA's Mandarin, Cantonese, Uyghur, and Tibetan Web sites have a unique connection to the people who live under Chinese censorship. They match rigorous reporting with lively interactive exchanges with their readers via email and message boards. Through cyberspace, as much as through the broadcast airwaves, RFA bears witness to the hope and despair of those who seek to exercise their right to free expression in China.

Audience research figures from Intermedia, an independent research firm, show there may be as many as 175 million adults in China accessing the Internet on at least a weekly basis, nearly as many as in Japan and South Korea put together. But the Web carries its own dangers. When Chinese readers go online, they do so under surveillance and often at great risk to themselves and their families. Rarely do they get a full picture; many sites are blacked out whether the users know it or not. The pages they visit are recorded, the content filtered, and their browsing patterns closely scrutinized. And the situation is not about to improve, as China continues to invest in the most advanced technologies for blocking unwanted material from blogs, emails, and Web sites.

The scope of China's Internet surveillance is daunting. Reliable figures are scarce, but reports speak of tens of thousands of Web police patrolling cyberspace, with 86 journalists or Internet users in Chinese jails. Beijing has enormous resources directed towards Internet censorship.

Conventional wisdom has long held that the open nature of the World Wide Web and its free, accessible brew of cultures would "bring democracy to China." Today that view looks optimistic indeed. The question is not whether the Internet is going to change China, but rather how much China is going to change the Internet.

RFA bears the brunt of Beijing's censorship. If RFA is stymied, its Chinese readers are deprived of news that is immediately relevant to their daily lives. They lose a chance for the crucial input that can help them make informed decisions for themselves and their families and form opinions based on accurate and balanced information.

As a news organization, RFA operates in a highly unusual environment and maintains a unique relationship with its Web users. RFA must not only distribute its news, but must help its readers to outsmart the censors. We know we are catering to people who might have to read the pages using proxy servers or via encrypted transmission services.

We use all available avenues to reach out to new readers and strive to stay at the cutting edge of technological innovation. Our radio broadcasts educate our target audience on how to use proxy servers and other gateways. On the Web, we offer live streaming of our broadcast shows. We are constantly looking for ways to evade the Chinese censors. In October we started offering our news programs via podcast to multiply the number of distribution channels and make the content ever more portable.

The Internet anti-censorship program of the Broadcasting Board of Governors provides support for our efforts to break through the Chinese blockage of our Internet content. The BBG's Office of Information Systems and Technology works with industry and government consultant experts to find ways to keep information flowing to China through Internet portals. The emails are distributed by BBG to users in China, which in turn allow those users the ability to access RFA, VOA or other blocked sites on the worldwide web through the proxy sites identified in the emails. The BBG continues to monitor and utilize the latest technology to get through the filtering mechanisms of the Chinese Government.

By all evidence RFA Web users are not easily deterred. They share their fears openly about being observed and even threatened by the Chinese government. One of our Tibetan readers wrote on a message board last month how he drew a menacing reaction when he posted "10 famous sayings for 2005 by Chinese leaders." "When I checked back," he said, "I received a threat from what I believe is a Chinese user. This showed how little China has changed over the last 50 years." But

others wouldn't let him get discouraged. "Don't be intimidated," answered one of his message board buddies. "We are practicing free speech. Whoever wants to intimidate those who speak out will be condemned and lose the moral high ground."

RFA is also partnering with a courageous and growing online community of technical experts inside and outside China who help us get our newsletters out to the people who need them. With their help, we are creating a widening network of human proxies, so informal that it has no visible shape but is very much alive. Message boards, emails, blogs and instant messages pick up where the government has cut us off. Friends and family based in third countries post our articles on their own Web sites and then pass on the Web address. RFA news travels fast and well by fax, letters, phone, and word of mouth. We know that when it matters most, our information gets to its destination.

The hope of the Internet for societies such as China's is that it will help enable people to communicate and hear dissenting views through a medium that is more anonymous, and hence leaves them less vulnerable to government retaliation. In the case of China, democracy activists, rights defenders, and others with a degree of computer literacy are increasingly using the Internet to exchange ideas despite the fact that in exercising their digital rights they risk incurring the wrath of the country's cyber-police. This is no doubt one reason for the recent highly publicized demand by Chinese authorities that foreign technology companies agree to limit their search engine functionality as a condition for operating within China. The Internet in general and online forums in particular are critical to the growth of rights consciousness and a freer civil society in China.

In addition to reporting on issues such as the jailing of cyber-dissidents and the closures of Web sites, RFA.org has increased substantially its coverage of specifically Internet-related and Internet-driven topics. Our Mandarin service news scripts are sent to more than two million e-mail accounts a day across China. Our February 1 report on US internet technology companies and China apparently struck a nerve with our audience, as it drew almost three times the number of page views that we witness on a normal day. The posting of the "Wild Pigeon" fable on our Uyghur, Mandarin and English web pages brought to thousands of people inside and outside the Uyghur Autonomous Region the allegory for which the poet and the publisher were imprisoned. The RFA Tibetan site has become a discussion forum for 164 topics of debate among Tibetans over the last 11 months and is now a real-time conduit for breaking news.

We are witnessing a profound change in China. That change is occurring not only in the economic and technological sectors, but even more importantly in the psychology of the Chinese people. Thanks in part to the flow of information that the Internet has facilitated, a growing number of socially aware Chinese have become loyal listeners of foreign broadcasters. At the same time, there has been an upsurge in rights consciousness on the part of the general public. As a result, people are less willing to live in obedience, and some are taking to the streets to voice their objections to issues ranging from forced evictions to corruption to environmental pollution. The Chinese Ministry of Public Security reports 87,000 public disturbances across the country last year, up from 74,000 the year before.

Radio Free Asia takes great pride in its high-quality work, and in the fact that we provide our listeners across China, and those in the other East Asian nations to which we broadcast with objective and balanced information. As such, we serve as an example of a free press for our listeners.

In addition to bringing news and information to the Chinese people that they cannot otherwise access, Radio Free Asia, through news analysis and commentaries, aims to promote Internet freedom by impressing upon its audience that human rights include digital rights, and that freedom of expression in real time—in the actual town hall or in the virtual town square—is itself a fundamental right, as enshrined in Article 19 of the Universal Declaration of Human Rights.

Conclusion

In conclusion, I would like to reiterate that Radio Free Asia is ably and eloquently fulfilling its mission-providing journalism of the highest standard to East Asian populations whose governments aim to restrict their access to full, balanced, and objective news coverage. RFA, further, is taking maximum advantage of Web technology to deliver our reporting by every available means, including RSS feeds and podcasting. Every day is a new race for technological advantage at speeds too fast to handicap—and with some notable victories.

Nearly a year ago, thanks in part to pressure from this Congress, Uyghur activist Rebiya Kadeer was released from jail in the Xinjiang Uyghur Autonomous Region and exiled from China. On March 17, 2005, she was reunited with her husband in the United States. RFA recorded the moment in words and photos that we quickly

posted on our Uyghur- and English-language Web pages. Barely 24 hours later, the children Ms. Kadeer had left behind in Urumqi had seen RFA's online coverage and excitedly told their siblings in the United States: "We saw our parents kiss!" In a Chinese autonomous region with uniquely stringent Internet controls, where police keep close tabs on who speaks to whom, where any Uyghur jubilation prompts suspicion or worse, this simple digital photo of Rebiya Kadeer and her husband locked in a tender embrace, published online from half a world away, constituted a joyful triumph.

Mr. SMITH OF NEW JERSEY. Ms. Liu, thank you so very, very much, and thanks for sharing that story. That shows you the power of a picture; particularly a picture of that magnitude; thank you.

Mr. Qiang.

TESTIMONY OF MR. XIAO QIANG, DIRECTOR, CHINA INTERNET PROJECT, UNIVERSITY OF CALIFORNIA–BERKELEY

Mr. QIANG. Mr. Chairman, my name is Xiao Qiang. I am the Director of the China Internet Project at the Graduate School of Journalism, University of California at Berkeley.

In the 12 preceding years, I also served as Executive Director of Human Rights in China. I have testified in front of this Subcommittee many times, including on the Tiananmen Massacre. I applaud your leadership on human rights in U.S. foreign policy.

Three years ago, I decided to assume a new challenge and have been exploring the digital communication revolution and how it has affected China's ongoing social and political transformation. It is my privilege to testify in front of this Committee again.

Let me start with a personal story, one of the most unforgettable experiences in my years as a human rights activist. In November 1992, an oceanographer in Seattle called my office at Human Rights in China after finding a bottle that had been drifting across the Pacific Ocean for 11 years.

A leaflet inside contained the information about Wei Jingsheng. Until the contents of the bottle arrived on my desk in New York, the world had not heard anything about Wei since 1979 when he was sentenced.

Well, 14 years later, we need not rely on a message in a bottle to receive news from inside of China. The country is continually opening to the outside world, with an exploding Internet population of over 110 million, and a booming high tech industry. China is now a member of the World Tarde Organization, and will host the 2008 Summer Olympic Games.

But what has not changed is the one party authoritarian rule of the Chinese Communist Party. Today's China has no fewer political prisoners than 14 years ago, including an increasing number of individuals who express themselves online.

There are a number of people in the past who have testified about the censorship mechanisms in China. I, myself, have given my written and oral testimony to the U.S.-China Economic and Security Review Commission, in which I outlined four layers of China's Internet control. There is the law, the technology, the propaganda, and the self-censorship. I will not elaborate on these contents further in this hearing. But I will ask that my testimony be included in the written record.

Mr. Chairman, let me now go to the central question of this hearing: The role of United States information technology companies in China in China's censorship mechanism.

It has become painfully clear to the American public in recent months that some of this country's leading companies, including Google, Yahoo!, Microsoft, and Cisco, who are here today, have to a different degree, aided or complied with China's Internet censorship policies.

We are all familiar with the individual cases, which have been widely reported in the media, so I will not go into detail. But more important than the individual cases is the fact that the problems faced by a few United States information technology companies today in China have a real impact on their industry as a whole; not to mention the global condition of human freedom and dignity.

The challenge in front of us, Mr. Chairman, is to find a way to help these companies work in concert, perhaps with some of the world's great research universities, to establish a set of guiding principles for the entire information and communication and technology industry.

These principles, or standards and practices, should transcend individual companies' own relationship to any given market. In other words, to seek collective ways to find the ability to resist demands for information or technology that violate fundamental human rights.

These standards and practices should support and respect the protection of universal human rights. They should also reflect specific beliefs of the industry, such as open access to communication networks, promotion of free speech, and protection of the security and privacy of information. They should be subscribed to by the information technology companies on a voluntary basis.

These standards and practices should serve not only as a catalyst and a compass for corporate responsibility, but also as a clear outline for what these companies cannot do, that serves as a buffer when companies are operating in a political environment where freedom of expression is restricted.

Such defense mechanisms should include all possible means, from transparency to non-collaboration and even resistance, to help these companies avoid aiding in or colluding with human rights abuses.

Having a set of standards and practices is not enough, however. It will only be effective if processes are simultaneously set up to actively promote, implement, and monitor the standards. The information industry should also make the implementation of these standards and practices transparent. Congress, the media, company shareholders, universities, non-governmental organizations, and the public all have an important role to play in helping those corporations be accountable to these standards.

Developing such standards and practices will not be easy, and it is a process in which academic institutions can have an important facilitating role. Three university institutions: The China Internet Project of the Graduate School of Journalism of the University of California at Berkeley; the Berkman Center for Internet & Society at Harvard Law School; and the Oxford Internet Institute in the United Kingdom will initiate a set of public meetings and private

workshops with interested information technology companies in the coming months.

Our challenge is to find ways in which rigorous research and writing can constructively address this problem. We want to work together with industry leaders and other academic researchers to develop a set of lasting standards which are credible, consistent, and effective.

Mr. Chairman, in the last century, we all witnessed the numerous atrocities and destruction; but also the prevailing tide of human solidarity in the struggle for freedom. One of glorious battles was fought in South Africa, where the international community, including many United States corporations, stood behind the South African people's struggle against apartheid.

During that period, a great American citizen, Leon Sullivan, authored the Sullivan Principles to help the U.S. business community exercise their collective strength to defend fundamental values of human dignity.

Today, a similar struggle is unfolding over the Internet, including in countries such as my homeland, China, where the authoritarian government is battling to hold back the tide of the free expression of Chinese people. Ultimately, freedom will prevail as our planet becomes ever more interconnected and interdependent. I believe that, once again, American corporations have an opportunity to be on the right side of history. I thank you, Mr. Chairman.

[The prepared statement of Mr. Qiang follows:]

PREPARED STATEMENT OF MR. XIAO QIANG, DIRECTOR, CHINA INTERNET PROJECT, UNIVERSITY OF CALIFORNIA-BERKELEY

Mr. Chairman, respectful members of the subcommittee,

My name is Xiao Qiang. I am the director of China Internet Project at the Graduate School of Journalism, University of California at Berkeley. In the twelve preceding years I also served as Executive Director of Human Rights in China, and have testified in front of this subcommittee many times. I applaud your strong leadership on human rights in U.S. foreign policy. Three years ago, I decided to assume a new challenge and have been exploring the digital communication revolution and how it has affected China's ongoing social and political transformation. It is my privilege to testify in front of this subcommittee again.

Let me start with a personal story—one of the most unforgettable experiences in my years as a human rights activist. In November 1992, an oceanographer in Seattle called my office at Human Rights in China after finding a bottle that had been drifting across the Pacific Ocean for eleven years. A leaflet inside contained information about Wei Jingsheng, then China's most prominent political prisoner, who had been sentenced to fifteen years in prison in 1979. Until the contents of the bottle arrived on my desk in New York, the world had not heard anything about Wei since his sentencing.

Fourteen years later, we need not rely on fortuitous messages in bottles to receive news from inside the People's Republic of China. The country is continually opening to the outside world, with an exploding internet population of over 110 million, and a booming high tech industry. China is now a member of the World Trade Organization (WTO) and will host the 2008 Summer Olympic Games. But what has not changed is the one party authoritarian rule of the Chinese Communist Party. Today's China has no fewer political prisoners than fourteen years ago, including an increasing number of individuals who express themselves online.

Although the Chinese authorities acknowledge that China needs the economic benefits the Internet brings, they also fear the political fallout from the free flow of information. Since the Internet first reached the country, the government has used an effective multi-layered strategy to control online content and monitor online activities at every level of Internet service and content.

Over the last two and a half years, my China Internet Project in Berkeley has been researching and monitoring the censorship mechanisms in the People's Republic of China. I gave my written and oral testimony to the U.S.-China Economic and

Security Review Commission in April 2005 on this subject, in which I outlined four layers of Chinese Internet control: law, technology, propaganda and self-censorship. I will not elaborate on these contents further in this hearing.

Mr. Chairman, let me now address the central question of this hearing: the role of U.S. information technology companies in China's censorship mechanism. It has become painfully clear to the American public in recent months that some of this country's leading information technology companies, including Google, Yahoo!, Microsoft and Cisco, who are here today, have, to differing degrees, aided or complied with China's internet censorship policies, in order to gain a presence in the lucrative China market. We are all familiar with the individual cases, which have been widely reported in the media, so I will not go into detail. More important than the individual cases is the fact that the problems faced by a few U.S. information technology companies today in China have a real impact on their industry as a whole, not to mention the global condition of human freedom and dignity.

The challenge in front of us, Mr. Chairman, is to find a way to help these information technology companies work in concert, perhaps with some of the world's great research universities, to establish a set of guiding principles for the entire information and communication technology industry. These principles, or standards and practices, should transcend individual companies' own relationship to any given market. In other words, to seek collective ways to find the ability to resist demands for information or technology that violate fundamental human rights .

These standards and practices should support and respect the protection of universal human rights. They should also reflect specific beliefs of the industry such as open access to communication networks, promotion of free speech, and protection of the security and privacy of information. They should be subscribed to by the information technology companies on a voluntary basis.

These standards and practices should serve not only as a catalyst and compass for corporate responsibility, but also as a buffer for companies operating in a political environment where freedom of expression is restricted. Such defense mechanisms should include all possible means, from transparency to non-collaboration and even resistance, to help these companies avoid aiding in or colluding with human rights abuses.

Having a set of standards and practices is not enough, however. It will only be effective if processes are simultaneously set up to actively promote, implement, and monitor the standards. The information technology industry should also make the implementation of these standards and practices transparent and provide information which demonstrates publicly their commitment and adherence to them. Congress, the media, company shareholders, universities, non-governmental organizations, and the public all have an important role to play in helping the corporations be accountable to these standards.

Developing such standards and practices will not be easy, and it is a process in which academic institutions can have an important facilitating role. Three university institutions—The China Internet Project of the Graduate School of Journalism of the University of California at Berkeley; the Berkman Center for Internet & Society at Harvard Law School; and the Oxford Internet Institute in the United Kingdom—will initiate a set of public meetings and private workshops with interested information technology companies in the coming months. Our challenge is to find ways in which rigorous research and writing can constructively address this problem. We want to work together with industry leaders and other academic researchers and programs to develop a set of lasting standards which are credible, consistent, and effective.

Mr. Chairman, respectful members of the sub-committee,

In the last century, we witnessed numerous atrocities and destruction, but also the prevailing tide of human solidarity in the struggle for freedom. One of the glorious battles was fought in South Africa, where the international community, including many U.S. corporations, stood behind the South African people's struggle against apartheid. During that period, a great American citizen, Leon Sullivan, authored the Sullivan Principles to help the U.S. business community exercise their collective strength to defend fundamental values of human dignity.

Today, a similar struggle is unfolding over the Internet, including in countries such as my homeland, China, where the authoritarian government is battling to hold back the tide of free expression. Ultimately, freedom will prevail as our planet becomes ever more interconnected and interdependent. I believe that once again, American corporations have an opportunity to be on the right side of the history.

Thank you Mr. Chairman.

Mr. SMITH OF NEW JERSEY. Thank you so very much.

Ms. Morillon.

TESTIMONY OF MS. LUCIE MORILLON, WASHINGTON REPRESENTATIVE, REPORTERS WITHOUT BORDERS

Ms. MORILLON. Mr. Chairman, I would like to thank you for giving us the opportunity to present our testimony today, and thank you for taking the leadership on this very important issue. I will present a brief summary of views.

China's rising economic power should not mask the appalling state of freedom of expression in the country. The Chinese Communist Party's Propaganda Department strictly monitors and censors the media. Those who step outside the line drawn by the Party are dealt with harshly. China is the world's largest prison for journalists and cyber dissidents. As of today, it has 81 of them behind bars.

In countries such as China, where the mainstream media is subject to censorship, the Internet seemed to be the only way for dissidents to freely express their opinions. But thanks to some American corporations, Chinese authorities have managed to gradually shut down this "open window" to the world.

Most authoritarian regimes try to control what their citizens do and read online, but China is far and away the world champion. It was one of the first repressive regime to realize that it could not do without the Internet, so it had to be brought under control. It is one of the few countries that have been unable to strictly block and monitor all material critical to the regime, while at the same time expanding online facilities. How do they do it? This is a clever combination of investment, technology, and diplomacy. Beijing has spent the equivalent of tens of millions of dollars on the most sophisticated Internet filtering and surveillance equipment. The system is based on a constantly updated Web site blacklist. The regime is also able to ban access to Web sites containing dubious key words or a combination of words such as "Tiananmen" or "massacre." I am not going to tell more about it, because it has been already discussed here.

But just to give you an example, the regime can also censor online discussion forums almost instantly. We have conducted some tests in China. For example, a call for free election is going to last about 30 minutes on a discussion forum, to tell you how effective the system is.

Internet censorship is also secured by a set of rules and regulations, and by harassing and tracking down cyber dissidents, the police are forcing Internet users to resort to self-censorship.

But authoritarian regimes like China's are getting increasingly efficient at blocking objectional material, usually with technology, but from Western firms. Some of these companies, most of which are Americans, do not respect freedom of expression while operating in a repressive country.

We have talked about Yahoo!, Google, Cisco System. I am not going to tell this again. I just wanted to tell how shocked we were when Yahoo! decided to hold that as on Shi Tao Weneegi to the Chinese authorities. It is one thing to turn a blind eye on human rights abuses. It is quite another one to collaborate.

We believe that these practices violate international law and the right to freedom of expression, as defined in Article 19 of the Uni-

versal Declaration of Human Rights, which is supposed to apply to everybody, business corporations included.

Some of these companies tell us that what they do is merely complying with local laws. Obeying local laws in a democracy such as the United States is fine. It is even recommended. Obeying the law in China is different, because the law is not done to protect freedom of expression.

When these companies overlook a Court order, they are, at the same time, violating the Chinese Constitution which protects freedom of speech. Furthermore, such ethical failings on the part of American companies damage the image of the United States abroad.

Internet companies were created to facilitate information access for all. Yet, some of them now find themselves in the awful position of collaborating with Web censors. They are altering the very natural product they are selling. By collaborating with repressive regimes censorship policies, they are helping to create country-specific access to multiple versions of the Internet. They are putting borders on this universal arena of communication that the Internet was intended to be.

The Internet is used in China to channel and influence public opinion, especially in support of nationalistic sentiments. As a state media, it is also used to promote Communist Party propaganda and to undermine the country's enemies.

Some Chinese media fuel anti-Americanism. For example, Xinhua, the state news agency, distorts facts, blasts China's enemies, and supports the world's worst regimes through its treatment of international news. But many assert that uncensored information in China would have significant internal impacts.

Internet censorship in China also subverts United States diplomacy efforts to promote democracy in the world. In helping Chinese authorities to crack down on dissidents and to control the free flow of information online, some IT companies are indirectly helping to block political changes in the country; thereby preventing China from following the path to democracy.

The future for online freedom of expression in China does not look good. China purchases the latest censorship technology from Western companies, and has more resources than counter-censorship efforts in the United States.

Reporters Without Borders of the Cisco, Yahoo!, Microsoft, Google. We also alerted the shareholders of these companies. And last November we presented a joint statement of 25 investment firms managing some $21 billion in assets. And these investment firms agreed to monitor the activities of Internet companies operating in repressive regimes.

Aside from Google, all the companies we approached refused to enter into a dialogue on the subject. Cisco reacted only last November after one of our statements was covered by the media. But today, thanks to media and congressional attention to these issues, some of these companies are starting to consider the consequences of their activities in repressive regimes as shown by the statements in the last days. This positive development is to be now followed up by concrete action.

Reporters Without Borders welcomes the creation of the Global Internet Freedom Task Force which shows how the U.S. Government is taking now seriously this issue. We are looking forward to knowing more about how it is going to work and which issues it is going to address. But Congress also has to formally take up this issue.

Reporters Without Borders is basically proposing six concrete ways to make these companies behave ethically in repressive countries, including China. We also addressed these proposals to the European Union and to the OACD because this situation concerns not only American companies but companies all around the world.

Reporters Without Borders would favor a two-step approach. We would like a group of Congressmen to formally request corporations to reach an agreement among themselves on a code of conduct that would include recommendations I am going to detail later on. If these companies are not able to reach an agreement amongst themselves or if they are not able to do it within a reasonable deadline then we would definitely support the legislation that would include these practical proposals.

We have listed them according to the type of service or equipments provided by these companies because they do not exactly provide the same kind of service. For e-mail services we would like no American companies to be allowed to have e-mail service within a repressive country. Therefore, if the authorities of a repressive country want personal information about any user of a U.S. company's e-mail service they would have to request it under a U.S. supervised procedure which is one of the proposals you are also about to include in your Global Online Freedom Act.

For search engines, we would like search engines not to be allowed to incorporate automatic features of at least of protected keywords. Among these protected keywords we would like words which have "democracy" or "human rights" not to be banned.

For content hosts, same thing, we would like U.S. companies not to be allowed to locate their host servers within repressive countries and we would like content hosts not to be allowed to incorporate automatic features of these protected keywords.

For Internet censorship technologies we have two options: Either American companies would no longer be allowed to sell these kind of products of they would still be able to market this kind of software but it would have to incorporate at least protective keywords rendered impossible to censor when they are dealing with repressive countries.

Eventually for Internet surveillance technology and equipment we would like U.S. companies to obtain the express permission of Department of Commerce in order to sell these kind of products to a repressive country. So we are definitely in favor of an export control. Same thing for training in this kind of equipment.

To conclude, President Bush stated in his last State of Union speech that "far from being a hopeless dream, the advance of freedom is the great story of our time." It is time to act before the initiatives of some American IT companies further endangers the growth of freedom and democracy in China. It is time to act to prevent Internet users in repressive countries such as China from falling victim to a new kind of apartheid, a digital apartheid. Report-

ers Without Borders is ready to offer its assistance to you, to this Committee and to the companies on this very important issue.

Thank you very much.

[The prepared statement of Ms. Morillon follows:]

PREPARED STATEMENT OF MS. LUCIE MORILLON, WASHINGTON REPRESENTATIVE, REPORTERS WITHOUT BORDERS

Mr. Chairman:

Thank you for giving us the opportunity to present our testimony today and for taking the leadership on this issue.

China ranks 159th out of the 167 countries in the World Press Freedom Index released last October by Reporters Without Borders. China's rising economic power should not mask the appalling state of freedom of expression in the country. The Chinese Communist Party's Propaganda Department strictly monitors and censors the media. Those who step outside the line drawn by the Party are dealt with harshly. China is the world's largest prison for journalists and cyberdissidents: as of today, it has 81 of them behind bars.

Reporters Without Borders has been defending freedom of the press for more than 20 years. It has also been denouncing attacks on the free flow of information online for several years. In countries such as China, where the mainstream media is subject to censorship, the Internet seemed to be the only way for dissidents to freely express their opinions. But thanks to some US corporations, Chinese authorities have managed to gradually shut down this "open window" to the world.

Internet censorship in China

Most authoritarian regimes try to control what their citizens read and do online, but China is far and away the world champion. Although the number of Chinese Internet users has been growing since first connected in 1993—and now surpasses 100 million—freedom of expression is still heavily censored.

China was one of the first repressive regimes to realize that it couldn't do without the Internet and therefore had to keep it under tight control. It's one of the few countries that have managed to block all material critical of the regime, while at the same time expanding Internet facilities. How do they do it? Through a clever combination of investment, technology and diplomacy.

Beijing has spent the equivalent of tens of millions of dollars on the most sophisticated Internet filtering and surveillance equipment. The system is based on a constantly updated website blacklist. Access to "subversive" sites—a very broad notion that includes pornography, political criticism and those which are pro-Tibet or favor Taiwanese independence—is blocked at the country's Internet "backbones" (major connection nodes). But censorship doesn't stop there: the regime can automatically bar access to sites in which "dubious" keywords, or word combinations such as "tianamen" + "massacre," are spotted. The regime can also censor online discussion forums almost instantly. Beijing has even convinced the world's major search-engine companies to abide by its rules and remove all material offensive to the regime from their Chinese versions, making it easier for the Chinese government to control the flow of information on line.

Internet censorship is also secured by a set of rules and regulations aimed at filtering the Internet, keeping track of users and implementing enforcement of these restrictions.

Moreover, by harassing and tracking down cyberdissidents, the cyberpolice are forcing Internet users to resort to self-censorship. About 50 of them are currently in jail in China for expressing themselves freely on the Web by calling for free elections or promoting democracy.

US companies' collaboration with Web censors in China

Authoritarian regimes like China's are getting increasingly efficient at blocking "objectionable" material, usually with technology bought from Western firms. Some of these companies, most of which are American, don't respect freedom of expression while operating in a repressive country.

Here are some examples that have caused us particular concern:

- Since 2002, Yahoo! has agreed to censor the results obtained by the Chinese version of its search engine in accordance with a blacklist provided by the Chinese government. Yahoo! helped the Chinese police identify and then sentence to jail at least one journalist and one cyberdissident who criticized human rights abuses in China. Yahoo!'s Chinese division e-mail servers are located inside China.

- Microsoft censors the Chinese version of its MSN Spaces blog tool. Search strings such as "democracy" or "human rights in China" are automatically rejected by the system. Microsoft also closed down a Chinese journalist's blog when pressured by the Beijing government. This blog was hosted on servers located in the United States.
- All news and information sources censored in China have been withdrawn by Google from the Chinese version of its news search engine, Google News. Google also launched last January a China-based, Google.cn, that is censored in accordance with Chinese law.
- Secure Computing has sold Tunisian technology that allows it to censor independent news and information websites such as the one maintained by Reporters Without Borders.
- Fortinet has sold the same kind of software to Burma.
- Cisco Systems has marketed equipment specifically designed to make it easier for the Chinese police to carry out surveillance of electronic communications. Cisco is also suspected of giving Chinese engineers training in how to use its products to censor the Internet.

Consequences of these ethical failings

We believe that these practices violate international law and the right to freedom of expression as defined in Article 19 of the Universal Declaration of Human Rights, which was proclaimed by the United Nations when it was founded and which is meant to apply to everyone—business corporations included.

Furthermore, such ethical failings on the part of American companies damage the image of the United States abroad.

Internet companies were created to facilitate information access for all. Yet some of them now find themselves in the awkward position of collaborating with Web censors in an effort to alter the very nature of the product they are selling. By collaborating with repressive regimes' censorship policies, they are helping to create country-specific access to multiple versions of the Internet. They are putting borders on this universal arena of communication that the Internet was intended to be.

The Internet is used in China to channel and influence public opinion, especially in support of nationalistic sentiments (see the "CRS report for Congress" of November 22, 2005). As the state media, it is also used to promote Communist Party propaganda and to undermine the countries' "enemies." Some Chinese media fuel anti-Americanism. Xinhua, the state news agency, distorts facts, blasts China's enemies (especially the United States and Japan), and supports the world's worst regimes through its treatment of international news. In addition to greater political openness and freedom of expression for the Chinese people, many assert that uncensored information in China would have significant international impact.

Internet censorship in China subverts US diplomacy efforts to promote democracy in the world. In helping Chinese authorities to crack down on dissidents and to control the free flow of information online, some US IT companies are indirectly helping to block political changes in the country, thereby preventing China from following the path to democracy.

The future for online freedom of expression in China does not look good: China purchases the latest censorship technology from Western companies and has more resources than counter-censorship efforts in the United States. The International Broadcasting Bureau for Counter-Censorship Technology spent more than USD 707,000 in 2005. But access to Voice of America and Radio Free Asia's websites has been blocked several times on the Chinese version of Yahoo and Google. These companies owe US taxpayers an explanation for how their money is being used to pay for the consequences of these firms' collaboration with China's censors.

Our previous initiatives

Reporters Without Borders has been writing to the CEOs of several corporations since 2002, proposing an exchange of ideas on this issue. None of our letters have been answered. We have also tried to alert the shareholders of these companies through their investment funds. On November 7, in New York, we presented a joint statement in which 25 investment firms managing some 21 billion dollars in assets agreed to monitor the activities of Internet companies operating in repressive countries.

Aside from Google, all the companies we approached refused to enter into a dialog on this subject. Cisco reacted only last November, after one of our statements was covered by the media.

Thanks to media and Congressional attention to these issues, some of these companies are starting to consider the consequences of their activities in repressive re-

gimes, as shown by their statements issued in the last days. This promising development needs to be followed up by concrete action.

Recommendations

Reporters Without Borders proposes six concrete ways to make these companies behave ethically in repressive countries, including China. These recommendations are being presented to the federal government and US Congress because all of the companies named in this document are based in the United States. Nonetheless, these proposals concern all democratic countries and have therefore been sent to European Union officials, as well as to the Secretary General of the OECD.

Reporters Without Borders is convinced that a law regulating the activities of Internet companies should only be drafted as a last resort, and we therefore recommend a two-step approach. Initially, a group of Congressmen should formally ask Internet corporations to reach an agreement, among themselves, on a code of conduct that includes the recommendations we make at the end of this document. The companies would be urged to call upon freedom of expression organizations for help in drafting the document. The request would include a deadline for the companies to submit the draft version of the code of conduct to the congressmen concerned.

In the event that no satisfactory code of conduct has been drawn up by the stated deadline, or the proposed code has not been accepted by a sufficient number of representative companies, the congressmen would set about drafting a law that would aim to ensure that US companies respect freedom of expression when operating in repressive countries, or elsewhere.

Reporters Without Borders' Proposals

We have listed our recommendations according to the type of service or equipment marketed by Internet companies:

- *E-mail services:* No US company would be allowed to host e-mail servers within a repressive country.[1] Therefore, if the authorities of a repressive country want personal information about any user of a US company's e-mail service, they would have to request it under a US-supervised procedure.
- *Search engines:* Search engines would not be allowed to incorporate automatic filters that censor "protected" words. The list of "protected" keywords such as "democracy" or "human rights" would be appended to the law or code of conduct.
- *Content hosts (websites, blogs, discussion forums etc):* US companies would not be allowed to locate their host servers within repressive countries. If the authorities of a repressive country desire to close down a publication hosted by a US company, they would have to request it under a procedure supervised by US judicial authorities. Like search engines, content hosts would not be allowed to incorporate automatic filters that censor "protected" keywords.
- *Internet censorship technologies:* Reporters Without Borders proposes two options:
  - Option a: US companies would no longer be allowed to sell Internet censorship software to repressive states.
  - Option b: They would still be able to market this type of software but it would have to incorporate a list of "protected" keywords rendered technically impossible to censor.
- *Internet surveillance technology and equipment:* US companies would have to obtain the express permission of the Department of Commerce in order to sell to a repressive country any technology or equipment that can be used to intercept electronic communications, or which is specifically designed to help the authorities monitor Internet users.
- *Training:* US companies would have to obtain the express permission of the Department of Commerce before providing any Internet surveillance and censorship techniques training program in a repressive country.

Note: The purpose of these recommendations is to protect freedom of expression. They in no way aim to restrict the necessary cooperation between governments in their efforts to combat terrorism, pedophilia and cyber crime.

[1] A list of countries that repress freedom of expression would be drawn up on the basis of documents provided by the US State Department and would be appended to the code of conduct or law that is adopted. This list would be regularly updated.

Conclusion:

As US Secretary of Defense Donald Rumsfeld stated last October, stressing the importance of political freedoms in China: "Every society has to be vigilant against another type of Great Wall . . . a wall that limits speech, information and choices."

President Bush stated, in his last State of the Union speech, that "far from being a hopeless dream, the advance of freedom is the great story of our time."

It's time to act before the initiatives of some US IT companies further endanger the growth of freedom and democracy in China. It's time to act to prevent Internet users in repressive countries such as China from falling victim to a new kind of apartheid, a digital apartheid.

Reporters Without Borders is ready to offer its assistance to you, to this Committee and to the companies on this important issue.

Mr. SMITH OF NEW JERSEY. Ms. Morillon, thank you very much for your testimony. And thank you to Reporters Without Borders for not just speaking out for journalists and cyber dissidents wherever they may be incarcerated or mistreated, but for being an incubator of many ideas that we are now trying to get enacted into law. So thank you so very much for that.

Ms. MORILLON. Thank you.

Mr. SMITH OF NEW JERSEY. Ms. Hom.

TESTIMONY OF MS. SHARON HOM, EXECUTIVE DIRECTOR, HUMAN RIGHTS IN CHINA

Ms. HOM. Thank you, Mr. Chairman. Thank you for inviting Human Rights in China to testify at this important and timely hearing. And I would note that, Mr. Chairman, you are the only one for the whole day of a very long day who has had no break, and that would also mean no lunch. So thank you for staying through the whole day to hear the last panel.

Human Rights in China has been actively engaged in individual case advocacy on many of these cases that have been noted today and education and research for almost 17 years. For the past 3 years we have been engaged in a pilot project called E-Activism that has been successfully challenging China's state-of-the-art censorship and surveillance system. We welcome this opportunity to share some of our insights and recommendations drawing on some of this hands-on experience.

I wanted to start with the observation that, if any of our corporate colleagues are still in the room, that as NGOs, governments and the business community we actually share the same stated norms and values. These are transparency, openness and fairness. In some ways you might say that human rights, NGOs and the IT companies are in the same business, except we are not profitable. We are in the information business, the business of generating, promoting and disseminating information because we do share the belief that knowledge is power. The Chinese propaganda, social and police and security apparatus know this very well.

There has been a lot of discussion today, and I would like to just have my written statement entered in the record and take my oral time to comment and to expand on some of the comments that we have been hearing today. There is a lot of discussion about China in transition. And certainly when I was living in China in the eighties and have returned every year until last year there have been some big changes. And in some other ways it has not changed. So I wanted to underscore that China is not monolithic either in the changes underway nor in its government.

My own personal experience in June when I was a formal member of the EU government delegation to China in Beijing at the EU-China Human Rights Dialogue, with an official visa from the Ministry of Foreign Affairs, yet that didn't stop the Beijing state secret police from deciding that it was time to have a friendly chat with me and decide that perhaps it took eight of them to come to my hotel room at night. And it was largely due to the intervention of the U.S. Embassy that I think I was able to safely leave China but I also had a very interesting chat with them. So I think that is important to keep in mind that the Chinese Government is not monolithic.

Secondly, it is not only about China changing but it has also been about the impact of China not only repressing at home but the efforts to expand its impact in the world. China was very active and vociferous in trying to silence this baby NGO, Human Rights in China, at the World Summit on Information Society. And it was the leadership of the United States Government, the Canadian Government and the EU Government that really challenged and had the unprecedented move of a 3-hour floor debate of which they tried to not mention our names but they said certain NGOs backed by certain governments, etc., etc., and then glaring at the U.S. Government. So it was quite clear what was going on.

So more is at stake than repression in China, which is very serious, but it's also the impact of China on the world and on multilateral processes and institutions.

Secondly, in addition to freedom of expression, access to information, it's important to keep in mind that the general human rights situation in China has deteriorated, not only for individual dissidents, it has deteriorated for the vast majority of Chinese people. That is documented by our reports, by NGO reports, by UN reports by the U.S. Government reports. And that is important in light of certain Members of the Committee who were concerned about needing to feed 1.3 billion people. Well, the Chinese Government are not doing a very good job of feeding or housing or providing healthcare for those people when we think about 700 million rural inhabitants without basic healthcare, 240 million at least migrants without housing or affordable jobs. So I think that is important to keep in mind.

So now two points. On the Internet and technology, and forgive the military use of dual use, but I think these are human tools, these are not technology tools. These are human tools with a dual use. And they are only substantively exnostic, that is the word, if you ignore the context. They are only substantively neutral, the technology, if we ignore the context and we ignore the predictable consequences of their deployment and application given a known, well-documented repressive legal, social and police infrastructure. And they are only neutral if we ignore the participation of the industry in actively seeking access into selling the software and the equipment.

I wanted to just add on Harry's comment about the China police both backwards and forwards. In the last China Police Exhibition at which this kind of surveillance, communication and transportation technology was sold, 90 percent of the exhibitors went home with a contract, including many United States companies. The next

exhibition, it is called China Police Exhibition, will be in 2006 in June on the anniversary of June 4. And I would hope there is some greater attention to this year's exhibition and the participation of all of these companies than has been in the past exhibitions.

So the tools of the Internet and the technology these can empower Chinese activists, journalists, rights defenders, intellectuals and grassroots groups, but as clearly has been shown today they are powerful tools of censorship and surveillance.

One note that has not been commented on today is that the rapid growth from 1998 to the present of less than 1.1 million users to over 110 million and counting this also reflects a very sharp digital divide, the haves and the have-nots. Not everyone is wired. Out of that it reflects the economic and social, the really growing economic and social gap that is fueling the rising social protests which is destabilizing China, which even the regime is now beginning to acknowledge. So there is a great social and digital divide.

The crackdowns on the Internet cafes, therefore, has a disproportionate impact on poor, migrant and rural populations who log on because they neither have the electricity nor the computers nor the homes to put a computer. We conducted a survey of nine provinces and about 70 cafes, and it is in our testimony and I won't go into that now, but the key question is not only to look at who is already online but if we are going to talk about access let us talk about access for everyone.

What information would Chinese access if they could access, and not so hypothetically? Let me share a little bit of what they access when they come to us. Following the launch of our E-Activism Project we went from less than—growing to almost less than 10 percent, the signatures from inside China to the Tiananmen Mothers' Fill the Square petition, this is because they are not allowed in Tiananmen Square, so they put a virtual bouquet in honor of what happened in 1989, it went up almost 40 percent. That is, when they had the access. It is not another time. People in China and the mothers of those students who will never come home are still demanding the truth and they want some accountability. Forty percent of the signatures are coming after we were able to give them proxy access.

The other, since 2003 we have been delivering proxy links to about 300,000 a week. We have been getting in about 76 percent successfully to the first SMTP level. Over the past 18 months the unique IP users has increased sixfold from 28,000 to 160,000. So if you think about those unique IP addresses at a computer it is not a one-to-one. It could be at an Internet cafe, it could be at a home, it could be at an office, it could be at a government level. So if you think of a conservative one to ten, the number of individuals, human beings who are accessing is probably well over a million, more than, only closer to 2 million.

Well, what are they going to look at? Our traffic analysis confirms that the Chinese readers are visiting the HRIC sites to obtain sensitive information that is not available from other sources. It is true the majority of the people online who are demographically young, male and educated and in the cities, are "Eat Drink Man Woman" and on the blog sharing their diaries, etc. However, what we have seen is over time there is a correlation between the Chi-

nese readers' efforts to obtain sensitive information and during periods when the government has really cracked down, every anniversary of June 4 there is a crackdown.

So Chinese want uncensored information, certainly the Chinese people who do want that. So the question is not as been posed repeatedly today and to have some comfort that it is inevitable that democracy and openness will come with the presence and engagement of foreign governments or the foreign companies, the real question is, yes, the change will come but what are the human costs and what is happening to the human damage while this is happening?

In terms of the role of the American IT companies in China the presence of them doing business we have to admit and we do acknowledge—presents very knew and complex human rights, business and corporate social responsibility issues. What has been clear today that they have been engaged in censorship, they have been engaged in content surveillance, Internet, etc. All of that I will not repeat because that has all been said today.

We also think the issue is not as been posed, whether they should be doing business in China, but how they do business and under what relevant guidelines. Really no one has the silver bullet, no NGO, no company, no government. But the first step is to acknowledge the tradeoffs honestly rather than to—it was a painful experience to listen to the justifications.

The engagement and presence in the Chinese market will not lead to any particular result except for market access for the companies. Corporate engagement and presence in China will contribute to greater reform but only if it is responsible and coherent. Vague, abstract, inaccurate, incomplete references to Chinese law in compliance with domestic law is indefensible for undermining human rights. We want to suggest that the obligations of the company need to be viewed in light of a coherent framework, that is, legal and ethical and that includes the laws of the home country, that would be the United States, the host foreign country, China, and the larger framework of international human rights obligations of trans-national companies.

Specifically, there has been a whole record of two decades of these efforts of codes but, more importantly, the recent UN norms on the human rights obligations which has garnered broad support and specifically lay out that the companies have two kinds of obligations, negative, to not be complicit in undermining human rights, and a positive obligation to promote. And they say that the companies have specific rights obligations that fall within their specific spheres of influence. And that means companies that are engaged in providing hardware, software, services or connectivity have a different opportunity and a different challenge. And we would urge both the Committee and the companies to look more closely at existing norms so that we're not starting from scratch.

The last point about the companies is that I would like to take a very different comment on the trade debates and the PNTR reference although that is a done deal. However, the partnership efforts of business and government throughout the very long process, more than a decade of the negotiations around China's WTO accession, is a useful example of what can be done instead of what hap-

pened here which was everyone was surprise by the predictable results of what happened when they entered and the way in which they entered.

Instead of passive complicity with existing law, no company, no sector, no government was willing to enter the Chinese market as it existed and under the existing law. Instead we had major demands and lobbying and negotiated for changes to Chinese law, changes to Chinese procedure, changes to Chinese values to facilitate the interests of business and foreign government. And that is exactly what happened. Following China's entry the U.S. Government and foreign governments have continued to promote both the necessary legislative changes with extensive intervention in the Chinese system. So I wanted to say that as an example that is absolutely possible.

Three sets of very quick recommendations. The solution is not technology guerilla warfare. We would like to urge not to go into the guerilla warfare, not to throw resources on both sides so that we have a new kind of star wars but if they do surveillance we do countersurveillance, etc. That is necessary in the short term. But in the long term the real question, the real solution is what was really alluded to by Ambassador Gross and Mr. Keith in their opening statements this morning which is that we really need to promote the change within China and for the journalists and the activists and the grassroots organizations who are working within China, that is where it is going to happen.

Well, how might we do that? First, compliance with Chinese law and promoting of rule of law. The U.S. Government has been very active in promoting a rule of law through the capacity building and the exchange programs, many of which I have been involved in, and through its political and human rights dialogue at various levels of formality. We want to suggest that the problems of the lack of a functioning legal system are widely recognized. These include a lack of an independent judiciary, the role of the party, the political committees in every single port which actually determine the outcome before trial, before the beginning of the process in sensitive cases and widespread corruption. We commend that widely-known documented fact to the companies when they think about compliance with Chinese law what kind of legal system we are really talking about there, not a functioning one.

The issues of Internet freedom, censorship, surveillance, including these individuals, must remain high on the agendas of these initiatives. And the U.S. Government has been participating in the bilateral process in which we have also participated. And we urge the U.S. Government to continue to do so and to share the strategies with the other governments and not to get picked off one at a time in the bilateral process.

The Chinese domestic law must conform to international law. This has not been underscored enough tonight. There is Chinese law. There was a much heralded, much much fanfare given by the Chinese Government and echoed by the western press for Article 33, the Human Rights Amendment. Let us give that a little more play here. There was an Article 33 Human Rights Amendment that says the state respects and promotes human rights. And that is in addition to the existing freedom of the press, etc., etc.

The industry standards I think enough has been said. And there have been some very good suggestions by my NGO colleagues already echoed. I would only add that we would hope that corporate counsel exercise greater due diligence in assessing a much more nuanced and comprehensive legal analysis than clearly has been done. And that would include identifying the whole range of laws, not just the Internet laws, and the tensions and conflicts and how to address them.

Looking ahead, two quick points, the Olympics. The Olympics 2008 as we lead up it will really matter, where is the traction, how will there be some traction? It matters to China to have a clean, green Olympics. Yet, in addition to the media access that we hope will happen for all the media, the roundups and the detentions which unfortunately will probably also occur in "cleaning up" before the Olympics, surveillance and communication equipment is being sold now, is being vetted now to China. And this is all being built now. We urge that attention be given to the "post-Olympic use" of this surveillance equipment so that they are not being left to even strengthen even greater the technology of surveillance.

There, part of that in the lead-up to the Olympics in all of these initiatives should be a call for the release of all. There are now over 300 or 400 still detained from June 4 related offenses. And there are still in detention those for counterrevolutionary crimes which doesn't even exist as a crime. All the journalists who are in prison they all should be called for a release in the next couple of years related to this. The companies can have a role in this.

And then, finally, in working together I have a short request to make it public to the industry. In working together with NGOs we have developed last year and was published by the Center for Democracy and Technology a framework, a beginning framework for how we might think about best practices for the company. We think it is pretty sophisticated and it is built on the lines of user, backbone, etc., every level.

We invite them, we invite Yahoo!, Microsoft, Google and Cisco to join in a conversation with us about how to move it to an operationalizing it. However, Google did mention today under much questioning that there is a list compiled by Google based on its own search results. Many of the NGOs, both my colleagues here and also sitting behind us, the ONI initiative, the Open Network Initiative is engaged in a great deal of very important research. We have colleagues from the Berkman Center sitting in the room. I think all of us would be very interested in the interests of transparency a disclosure of that list. We would all like to know what are those sites? Can they disclose it on their Web site? Can you disclose it on the government Web site? It would help us understand how we can do our end of the battle which is to try to open the access. We would like to know what is being blocked as the whole universe. So that would be a very in the interests of sharing information.

Finally, we want to urge that you think beyond isolated technologies. That it was clear that has been alluded to in various ways today the technologies today should not ignore the challenges and the opportunities that are in the expansion into the collateral uses of surveillance or the restricted uses of the particular technology. And this is very clear now what we have now is the blur of a line

between online and offline technologies are getting much more interrelated, technologies such as Web browsing, voice-over IP, e-mail, instant messaging, SMS, pod casting, all of these are being developed by Web activists around the world and beginning in China in a very active way. And that is going to be the next arena and already has become the next arena for filtering.

So coming at the end of a very long day I want to thank you for your attention. And we do want to move forward in a constructive way. But perhaps I would like to end with the voice of not our voice, but since we have been talking about censorship perhaps just a quick two lines, three lines from the voice of someone whose blog was removed, and that would be Michael Anti. He published an open letter in Chinese which we think is very powerful and addresses many of the issues discussed today. Human Rights in China has posted an unofficial, of course, we posted an English translation of it on our Web site. It's at ir2008.org. But this is relevant.

> "Regarding the legislation by Members of the U.S. Congress this is completely a matter for the American people. I do not think that the U.S. Congress can protect Chinese people's freedom of expression. If the freedom of expression of citizens of a great country must be protected by the Congress of another country this demonstrates how remote our country is from the grandness of its ideals. To state it more clearly, what I need is legislation by the Chinese National People's Congress. What I need is Chinese people legislating to protect Chinese people's freedom of expression. If it can't be done today it certainly can be done tomorrow. This is the only honor and dream we live for."

And I think that is a task for the U.S. Government, for all the world's governments and for the industries: How do we enable the condition that will make this dream possible?

Thank you.

[The prepared statement of Ms. Hom follows:]

PREPARED STATEMENT OF MS. SHARON HOM, EXECUTIVE DIRECTOR, HUMAN RIGHTS IN CHINA

Mr. Chairman, thank you for inviting Human Rights in China (HRIC) to testify at this important and timely hearing.

As an international Chinese human rights non-governmental organization (NGO), HRIC has been actively engaged in individual case advocacy, education, and research for almost seventeen years. Over the past three years, HRIC has also accumulated experience in successfully challenging China's state-of-the-art censorship and surveillance system through our E-Activism pilot project. We welcome this opportunity to share our insights and recommendations.

NGOs, governments, and the business community share stated norms and values of transparency, openness, and fairness. In some ways, human rights NGOs and IT companies are in the same business, the information business, the business of generating, promoting, and disseminating information—because we share the belief that knowledge is power. The Chinese propaganda, social and police apparatus understands this very well.

THE INTERNET AND TECHNOLOGY—HUMAN TOOLS WITH DUAL USE

In China the Internet and technology are tools that can empower Chinese activists, journalists, rights defenders, intellectuals, and grassroots groups; they are also powerful tools of censorship, surveillance, and social and political control wielded by an authoritarian regime. From June 1998 to June 2005, the number of Internet

users in mainland China grew from 1.17 million to 103 million (China Internet Network Information Center, *16th Statistical Survey Report on the Internet Development in China*, July 2005, 50.) and according to the 17th CNNIC survey (http://www.cnnic.net.cn/images/2006/download/2006011701.pdf), now stands at around 110 million.

The rapid growth of online users also reflects a sharp digital divide: 91.69 million Internet users are in Chinese cities, accounting for 16.9 percent of the urban population. Only 19.31 million individuals, or 2.6 percent of the rural population, are online. Chinese officials recognize the problem posed by the digital divide for overall expansion: many villages in China only have one phone, personal computer prices are still too high for rural residents, and infrastructure development issues remain a high priority.

In light of this digital divide, the crackdown on Internet cafés in China also has a disproportionate impact on poor, migrant, or rural populations who log on in those cafés. In the summer of 2005, HRIC conducted *a field survey of Internet cafes* in over 9 provinces in China. HRIC field survey describes the availability and locations of cafés surveyed; software and hardware installed, including censorship and surveillance software and practices; and user demographics and ambiance inside the cafés. See HRIC, *Logging on in China's Internet Cafés*, CHINA RIGHTS FORUM, No. 3, 2005, 102–109 (http://ir2008.org/article.php?sid=58).

What information would Chinese users access if they could?

Following the launch of HRIC's E-Activism Project, the Tiananmen Mothers' Fill the Square online petition registered a dramatic increase in the number of online signatures from inside China. This, coupled with feedback from readers of the *Huaxia Bao* e-newsletter and traffic analysis of HRIC's websites, reflects mainland Chinese Internet users' desire to reach beyond the firewall and China's system of information control.

Since September 2003, HRIC has been delivering proxy links to the uncensored Internet with its Chinese e-newsletter to over 300,000 Internet users in mainland China. An average of 76% of all e-mails are successfully delivered to the SMTP layer. The newsletter's content is generated directly from mainland Web sites and Internet users. Over the past 18 months, the monthly average unique IP users to the e-newsletter's Web site has increased nearly 6-fold, from 28,000 to over 160,000 unique IP users.

Our traffic analysis confirms that Chinese readers visit HRIC's Web sites to obtain sensitive information not available from other sources. Over time, assessments have identified a correlation between Chinese readers' efforts to obtain sensitive information and specific periods during which government censorship has prevented access to other electronic news sources.

ROLE OF AMERICAN IT COMPANIES OPERATING IN CHINA

The presence of US-based IT companies operating in China presents new and complex human rights, business, and corporate social responsibility challenges, including those recently demonstrated by various companies' complicity in undermining freedom of expression, access to uncensored information, and the privacy rights of Chinese citizens. Today, even the Chinese government is citing the practices of these major companies as justification for their own censorship and information control. See Joseph Kahn, "China's top monitor defends Internet censorship," *The New York Times*, February 14, 2006.

US companies are engaged in censorship of online content, Internet search results, and disclosure of user information:

Online content: In accordance with the "Public Pledge of Self-Regulation and Professional Ethics for China's Internet Industry," companies, including Yahoo!, agree to remove any information considered harmful, or which may disrupt social stability from Websites that they host. These sites include blogs, such as that of Beijing investigative blogger Anti, which was shut down without warning by Microsoft on December 31, 2005. While Anti has reopened his blog on a US-hosted system, domestic readers will no longer be able to access it. See HRIC's Web resource providing an unofficial translation of Anti's response to proposed Congressional legislation on the obligations of U.S. companies operating overseas.
(http://ir2008.org/article.php?sid=138).

Individuals who subscribe to Yahoo! e-mail accounts in China are given a terms of service (TOS) agreement that differs substantially from the Yahoo! US and HK user agreements. The China user agreement holds users accountable for domestic laws proscribing content considered to endanger national security, including vague state secrets laws.

Internet search results: IT companies such as Yahoo!, Google and others filter the results of searches conducted in China, in compliance with Chinese government regulations. As a result, Internet users conducting searches on issues such as democracy, religion or human rights, will only be able to access pages with government-approved content. Several groups, including HRIC, have done comparative searches between Google.com and Google.cn, Google's new mainland China search engine. The results demonstrate the skewed results obtained by using search engines based in mainland China. See HRIC's Web resource, *Google.cn: Not too late for corporate leadership* (http://ir2008.org/article.php?sid=135).

Disclosure of information: The Yahoo! example is illustrative of the marginalization of relevant domestic Chinese law that protects privacy rights and freedom of expression. Article 40 of the PRC Constitution protects privacy of communications. However, as demonstrated by the case of jailed journalist Shi Tao, e-mail providers, including Yahoo!, have been complicit in convictions by disclosing personal account details during criminal investigations. See *HRIC Case Highlight on Shi Tao*, (http://hrichina.org/public/highlight/index.html).

The issue is not whether *US companies do business in China, but* how *they operate and what are the relevant guidelines.* No one sector has the silver bullet, but the first step is to acknowledge the trade-offs honestly rather than offer self-serving justifications. Engagement and presence in the market alone will not inevitably lead to any particular result except for market access for the companies. Corporate engagement and presence in China will contribute to greater reform and openness only if it is responsible and coherent.

Vague, abstract, inaccurate reference to "Chinese law" and compliance with domestic law is an indefensible justification for undermining human rights. The obligations of companies need to be viewed in light of a coherent framework of the legal and ethical obligations of IT companies that includes the laws of the home country, the host foreign country, and the larger framework of international human rights responsibilities of transnational companies.

The partnership efforts of business and government throughout the long process of negotiations around China's World Trade Organization (WTO) accession, are a useful example and precedent of what can be done. Instead of passive complicity with existing law, no company or government was willing to enter the Chinese market as it existed, under the existing law. Instead major demands were lobbied and negotiated for *changes* to Chinese law, to facilitate the interests of business and foreign governments. Following China's entry into the WTO, industry, business, and governments were and are active in promoting the necessary legislative changes, and closely monitor and assess China's compliance with its WTO obligations.

Beyond not being complicit in contributing to and legitimating Chinese government censorship, the business community and the industry has the same opportunity to exercise leadership in promoting greater openness, and human rights protections in China through their business practices, their lobbying, and support for legislative reforms.

RECOMMENDATIONS:

1. Compliance with Chinese law and promoting a rule of law in China:

- The challenges of developing a rule of law in China and a functioning legal system are widely recognized. These include: lack of an independent judiciary; the role of the Party and the politicization of decisions in sensitive cases; and widespread corruption. The U.S. government is active in promoting a rule of law in China through capacity building and exchange programs and through its political and human rights dialogues at various levels of formality. *The issues of Internet freedom, censorship, and surveillance, including the cases of individuals detained for exercising their freedom of expression, should be included on the agendas of these initiatives.* See HRIC's work on individual cases. (Shi Tao: http://ir2008.org/article.php?sid=71, Zhang Lin: http://hrichina.org/fs/view/downloadables/pdf/crf/CRF–2005–4__PrisonerProfile.pdf, Yang Zili: http://hrichina.org/public/contents/press).
- Chinese domestic law must also conform to international law, specifically to China's international obligations, including its human rights obligations. In fact Chinese domestic law includes provisions for protections of freedom of expression, press, privacy, and right to criticize the government. The PRC Constitution even includes a much publicized human rights amendment. Article 33 of the PRC Constitution states that the state respects and promotes human rights, while Article 35 guarantees citizens freedom of speech, the press, association and assembly. When assessing compliance with Chinese Law, corporate counsel should undertake a more nuanced and comprehensive

legal analysis that identifies specific laws, provisions, tensions or conflicts between different laws, and how to address these conflicts or tensions.

2. Developing Industry-wide standards that are specific and also draw upon international norms:

- IT Industry groups should adopt industry wide standards for doing business in countries with repressive regimes. However, unlike the general aspirational Code of Ethics promulgated by individual companies, industry wide standards are only effective if they are specific, include effective monitoring and reporting provisions, and are operationalized throughout the company. HRIC has also outlined a beginning framework best practices for IT companies doing business in China. See HRIC, *Human Rights and Spam: A China Case Study*, in SPAM 2005: TECHNOLOGY, LAW AND POLICY, Center for Democracy & Technology (http://ir2008.org/article.php?sid=57).
- With respect to disclosures of information, adopt an industry standard where companies only censor specific sites or other subpoenas, in compliance with relevant Chinese laws and regulations information, or hand over the personal information of their users, only when specifically required to do so by a legally binding notice from the government, such as criminal, including the Criminal Procedure Law (CPL). The CPL affords individuals the right to legal counsel and public trial, among other procedural protections.
- Under *The UN Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights*, TNCs have a special responsibility with respect to rights that fall within their respective spheres of influence. IT companies engaged in providing hardware, software, services, or connectivity, have different challenges and opportunities *to avoid being complicit in* human rights violations and *to promote human rights.*

3. Looking ahead: Beyond isolated technologies and towards 2008

- Preparations for the 2008 Olympics have attracted the participation of foreign companies across diverse sectors, including construction, advertising, architecture, legal services, surveillance and communications. The beneficiaries of the Olympic Games, and as such of the contracts agreed to between foreign companies and Beijing as the host city, have always been presented as the people of Beijing, and more broadly, of China. This is documented not only in China's numerous promises to the International Olympics Committee before being granted the right to host the Games, and also in its 2002 Olympic Action Plan. During the Olympics, security equipment and infrastructure will be operated by the government. How will the hardware and technical know-how be used after the Olympics? The post-Olympics use of this equipment and these technologies must be transparent and monitored. Given China's human rights record, what are the impacts on privacy rights if these technologies are exported to other countries?
- Any industry-wide code of conduct or specific legislation should move beyond the narrow conception that technologies are used in isolation of one another. *The lines between online technologies and offline actions have been blurred.* Technologies such as Internet Web browsing, VoIP, e-mail, instant messaging, SMS, podcasting, and more, work in interrelated spheres, impacting journalists, students, activists, organizations, and individuals in their access to and dissemination of knowledge.
- Any recommendations and guidelines should not ignore the challenges and opportunities that lie ahead in the expansion into the collateral uses of surveillance or the restrictive uses of a particular technology. For example, SMS messages will not only be increasingly filtered, but could also be integrated into database systems used to store and track required pre-paid cell phone user information, with serious implications for users who may send and receive politically-sensitive messages.

Coming at the end of a very long day, thank you for your time and attention to our testimony. We look forward to moving forward in a constructive way and an ongoing opportunity to exchange views and suggestions.

Mr. SMITH OF NEW JERSEY. Thank you for that very eloquent statement and to all of you for the tremendous work you are doing on behalf of human rights in China and in many cases other places as well in other repressive countries.

Let me ask just a few final questions before we conclude our hearing.

You know, I think your point, Ms. Hom, about the appeals to international law and how we need to be emphasizing not only as China's own Constitution being violated by these regulations but the Chinese Government has signed a number of internationally binding covenants, including the International Covenant for Civil and Political Rights. And I would note parenthetically that time and time again, especially in anticipation of a visit by a visitor to the United States from China, some new and seemingly step forward or progress on that very covenant would be announced to try to quell any kind of criticism that President Hu or Lee-Pong or, I don't know if he was here, but some of the other leaders who have come here. I met Lee-Pong myself when I was in China back in the early 1990s. But Article 19 could not be more clear of that UN document with regards to press freedom and basic freedoms of speech. So I think your point is very well taken there.

I have one question about whether or not the average Chinese who goes online really recognizes the trap that may be set for him or her as they send e-mails that they think are private, as they surf the net and type in prohibited words and phrases. I was again struck, and I said this to the last panel, by how all three of, well Google, Microsoft and Yahoo!, but especially Google and Microsoft spoke with great affection for the Chinese Academy of Social Sciences and a study that was recently done that found that one in, they said 54 or 60, I am not sure which it is, of the users believe the Internet provides more opportunities to criticize the government.

One, you know even in politics my friends on the Democratic and as well as the Republican side are always apprehensive about the validity of any poll. What were the questions asked, size of the sample, transparency, who did the collecting of data? And it seems to me that in this case we are talking about, I do not care who funded it, what was the contact, the interface if you will with the individual Chinese man or woman to garner and glean that information? And it seems to me that could easily be manipulated to show somehow so there is a great talking point here and everywhere else to say, well, look at this, people really feel they have, you know, an ability to criticize the government. Try doing it and next thing you know there is a knock on your door at 4 o'clock in the morning and it is off to the Laogai, as Harry Wu knows so well, having spent 19 years in that horrific place, where you will be tortured and maltreated.

And so what do you make of this? I got a sense that there was not even a sense of discomfort on the part of the previous panel that they may be getting additional information that they are now putting into testimony, advising their board when they talk about these issues, relative to this Academy of Sciences and this kind of data. What is your sense on that? Anybody like to? Yes.

Ms. HOM. Can I say something quickly about the international treaties?

Mr. SMITH OF NEW JERSEY. Yes.

Ms. HOM. In the earlier questioning by the Chair and by the Members of the Committee I was frankly shocked that the compa-

nies did not reference. There was a very quick, easy answer under international law. China has signed all of the treaties that you have correct—that you referenced. But the committee, the Convention Against Elimination of Racial Discrimination, which is broader than racial discrimination so discrimination, women, economic, cultural and social rights, all of these very clearly gave the international law answer which is that China was bound, that if the hypothetical, not so hypothetical to discriminate against women in China, no, you can't do it because they have signed on to international treaties which prohibit it.

On the ITCPR the ratification of the ITCPR has been promised ad nauseam and has been on the agenda for not one, not two, but at least three workshops with the EU to help them how to ratify. And the U.S. Government has also given them technical assistance on how to ratify. The ratification is not a mystery. The jurisprudence is very clear, and I would urge to push that. They have signed. They do not need to change all of Chinese law to be in compliance before they ratify. They did not change all of Chinese trade law before they acceded to the WTO. They entered the WTO and then they changed the thousands and thousands of law, which took years which is why they have a 4- to 5-year implementation stage. The same thing with the ITCPR, they should ratify it now.

Even without ratifying it they are still bound by the norms. They are not supposed to, having signed it, violate any of the basic principles and values including freedom of expression. So it is "binding."

On the "average Chinese," the CAS study we had taken quite a bit of public exception to it. The main part of it was to raise exactly, Mr. Chairman, the questions you raised. The methodology, the sampling, they were not defensible.

Secondly, the whole report did not contain one reference to one person in detention as a result of Internet activities. That was shocking. And when we raised that point they said it is because the focus of that study was not censorship. You cannot have a study that looks at whether the Internet will be a tool, etc.

On whether average Chinese know, I think that there is 1.3 billion. There's only 110 million online. We can't say what they all know. But I would say that it is probably different levels. The people who are very sophisticated on the blogs they are pretty aware of some of this stuff. The Internet activists they are pretty aware. The grassroots activists pretty aware. And they take their calculated risk. The lawyers, the rights defenders, the Weiquah movement, which is China's very exciting civil rights, it is their own civil rights movement is a way to think of it, they know some of the risks and they are taking calculated risks. And that is why they are very courageous.

However, ordinary Chinese might get on and they do not know that it is not about blocking, it is that stuff is getting through, that e-mail is getting through, it is being logged under a system in a server with Cisco helped and Nortel helped build, so that they are logging in all of this. And then when the evidence was eventually disclosed in some state secret and then eventually we find out it is e-mails, it is e-mails that were allowed to get through that were

filtered, that is the evidence that convicts the people. So some people do not know.

There is a lot of interest in the NGO community. And we have been having some conversations. And that is why we would very much like to be part of the ongoing steps to develop these toolboxes for Chinese who go online, not only to teach them basic Internet skills but they should have some higher level of awareness about the security risks and what to do about anonymity, what to do about the surveillance, how to protect themselves. That is not out there in Chinese. There are very good toolboxes developed by Citizens Lab, by the Berkman Center, they are all working together in very exciting initiatives. They need to be not just translated into Chinese, they have to be redone for a Chinese user. And that is what we can build on so that we can help it to be safer for them to access the Internet.

Mr. SMITH OF NEW JERSEY. Yes, Mr. Xiao.

Mr. QIANG. My project at Berkeley has been monitoring and researching the how Internet affects Chinese society for the last 3 years. So I say this with a close observation and a substantial study. Your question about the validity methodology of the CAS study is valid. It is extremely controversial and hard to do any objective valuable social science study in a political environment which manipulates information. But that being said, my research and my observation tells me Internet is a tool to positively opening the information in China. Chinese people more than ever are having more opportunities to criticize government, to express their opinions, especially on those less sensitive or more gray areas, but it is a great empowerment to them.

Ask any Chinese journalist, you ask any Chinese citizens they pretty much tell the same thing. It has also expanded their information environment. That is precisely why we see such an effort from the government trying to fight that, trying to control that, trying to suppress that. The effort, the extent the Chinese Government went to to censorship online is to highlight this, that is actually a great progress, a potential and a force of the Internet pushing Chinese society more politically open. So let us not confusing the two.

Secondly, your question about whether the Chinese user is aware of the trip, two points. One, that's not the way Chinese censors are thinking. Chinese censors are thinking they want to warn, intimidate every Chinese user to let them know they are always being monitored, they are always there. Actually, that is the strategy Chinese police are using.

They use search word "Internet police" in Chinese on the Chinese Internet. You have millions of Web site and pages mention that word because precisely the Chinese Internet police is not hiding, they want the people know that they are there. That is the strategy, and it works.

Secondly, you are also right about there are surveillance and tracking down technologies being used by Internet police to track down specific conversations or into the disinformation form that exist. But the dominant strategy is intimidation, is actually they make them explicit to the Chinese users.

Mr. SMITH OF NEW JERSEY. Ms. Liu?

Ms. LIU. I can add a couple illustrations. At RFA on our Tibetan-language Web site, a message board is one of the most popular features. At one point last year we asked our users to register themselves so that we could send them newsletters. Participation dropped to zero. So I would say the users are very aware of the risks.

Secondly, in my written statement I referred to a story we did about Guangdong Province in the city of Shenzhen. Some users wrote to us that there is a new Web police warning system being used there. Every time they log on this figure of two policemen pop up. If you click on the icon it takes you to a warning page that tells you, "warning: Internet users must comply with the law." The users that alerted us to this phenomenon told us immediately that they were intimidated. As soon as they saw the pop-up they were afraid. And they were certain that the pop-up was a surveillance tool.

So I think that Internet users are quite aware of the risks they take. And it is so incumbent on us to protect them.

Mr. SMITH OF NEW JERSEY. Yes, Mr. Wu?

Mr. WU. I just want to add one more comment. You know, the reason why these companies in China are so aggressive is because it is like a big cake. The Golden Shield, the Golden Shield program cost $6 billion. They want to occupy the market, okay. So Cisco, you see this guy, okay, he introduced the Cisco President Chambers when he visited China and was interviewed and had the opportunity to meet Jiang Zemin. This is a big cake. They want money. And the money has a smell like blood.

Mr. SMITH OF NEW JERSEY. Yes, Ms. Morillon.

Ms. MORILLON. Just wanted to add something. We have some Internet users in China that have found ways to bypass some of the restrictions and firewalls. But most of the Internet users are not Internet geeks and cannot use all the circumvention technologies, especially when you know that an analyzer that has come is blocked inside China. So most of the users are trying to use proxy servers but they are constantly blocked by the authorities so they have to change to find other servers, other proxy servers.

So it a constant fight between these people who are trying to circumvent censorship in China and the authorities that are constantly baiting their Web site like these technologies and everything. So that is definitely something that we need to go on working on.

Mr. SMITH OF NEW JERSEY. Let me ask you, in answer to questions with regards to Yahoo! Mr. Callahan talked about Alibaba and the fact that, you know, they basically don't have control over them. And I am wondering what do you think the moral culpability is of a United States company, or any company outside of China but especially a United States company, when they create a subsidiary like Alibaba and they are still major stakeholders in that company and yet it gives them kind of a plausible deniability, and I did ask him that earlier, to say, well, you know, they are local and we are over here.

It seems to me that that seeks to protest too much, especially when Alibaba, you know, is potentially providing all kinds of e-mails. We do not know because apparently that is against the law,

Chinese regulations and law as well. So we do not even have a sense of the parameters. And as he said, they found out after the fact that Shi Tao was under investigation. Now, you know I think there needs to be a suspicion any time a member of the public security police come in and say we want so-and-so's e-mail. For what? It is a legitimate reason for someone to ask? And were they lied to? Were they told it was some other kind of investigation?

So what about this idea of having other corporations that are China-based?

And secondly, it seems to me that Google and the technology that many of these United States corporations have developed really is the best of the best and that the Chinese search engines and the Chinese technology does lag. So there is a reason why the government, especially for dual use purposes, both military and police, would want to get its hands on this kind of technology sooner rather than later. So I am struck by this idea of, well, they will do it anyway and they will have their search engine. Yeah, and they will be much further behind what you have to provide.

So you know, you can negotiate from a position of strength. The terms and conditions that you accept do not have to be 100 percent or mostly on the side of what the Chinese want to prescribe for you to follow. What is your sense on those questions?

Yes, Ms. Morillon?

Ms. MORILLON. To answer the question about how much leverage they have with the authorities, yeah, I mean one of the most disturbing given from the company is to say either we collaborate, we comply with local law or we have to leave China. There is something in between. You can negotiate. And this has never been done. I mean these companies have negotiated one by one with the Chinese authorities. What we need now is them to put a united front and to go and negotiate with Beijing.

They are Internet giants. They cannot be ignored in their own segments. I mean when you look for information you Google it. Even when Google was censored in China it was still among the five leaders in search engines. So the first one is the Chinese search engine Baidu. But I do believe that these companies are giant, that they cannot be ignored, that they have real leverage in negotiations with the Chinese authorities.

And the other thing that I would like to add is that if the long-term goal of the Chinese authorities is not to have American companies being leaders on these markets. So if they are keeping American companies now it is because they still need them, otherwise they would have kicked them out of the country.

Mr. SMITH OF NEW JERSEY. Ms. Hom?

Ms. HOM. On Yahoo! I know that under tremendous difficult questioning the representative continued to say that they do not have daily management responsibilities. But according to Yahoo!'s own press releases, this is just to bring it to the attention, the long-term strategic partnership between Yahoo! and Alibaba was the first of its kind and it was a partnership model for an Internet company in China when it was announced in August 2005. This is information we now have, and they could correct it which we would welcome to hear.

The four-person board consists of Alibaba and the other directors are Jerry Yang, CEO of Yahoo! and co-founder, and a representative from Softbank. So it's a very small management board that is overseeing the joint operation. We are not talking about a huge operation.

Secondly, as an investor it is not just a large investor, it is a 40 percent economic interest investor and has 35 percent voting rights. So we are talking about not just any investor having no management oversight, we are talking about a substantial amount of shareholder power of 35 percent voting rights and a 40 percent economic interest. And that would in terms of responsible shareholder I think you have to exercise your shareholder rights.

The second thing I wanted to underscore is what Lucie just said is that there has been a change in China and in the last maybe 5 years almost China went from importing and buying technology, particularly at the high end, and they are now in a position in a very fast time frame exporting it. And that is the technology as well as the hardware.

A good question to pose to Cisco is, how much of Cisco equipment is now being produced in China? I would venture a guess to say very high, almost all of its actual productions are in China. They are not only in the router business they actually are producing them in China.

Secondly, in terms of training personnel, I understand just anecdotally that there are about 12,000 in the whole world Cisco certified engineers. Several thousand of them are here in the United States and the other highest core percentage is in China. So they are training the highest percentage of the engineers, I think it's like two, three thousand there, two, three thousand, I think it's roughly equal. And it would be good to get a clarification of that because a business doing business in China has many levels, training, personnel, transferring of culture, not just the selling and buying of the services. And I think that would be a good thing to get a clarification on.

In terms of operationalizing all the companies, for one thing it would be quite simple, they could start keeping records how many requests, that would be really simple. And that's a very simple—everything else is quite complex that we have talked about today. But keeping simple records in every company that would seem pretty reasonable to request, to say can we start doing that now? How many requests? How many police? And in the end how many turned out to be about pornography?

The ONI study very clearly showed in the scope of that study that the majority of the terms and the content filtered was not pornography, was not harm, was not that, it was political sites or democracy sites.

And the last thing, Mr. Chairman, I can share, there was a very curious item yesterday in the news which was in the *Washington Post* and also in the *New York Times* and also in some Chinese reported papers, the Chinese State Council Information Office gave a very unusual briefing of which they said something very that should not be lightly ignored. First they said we acknowledge we have the state-of-the-art censorship. But secondly, they did not claim Chinese exemption laws. They did not claim that China will

do what China does and you can't interfere. Instead they claim they were in compliance with international norms, international practice. And then, oddly and bizarrely, the companies today have all been saying to stay in China we have to do what the Chinese Government tells us to do. What the Chinese Government said yesterday was, you know why we can censor? Because the companies are doing it, because the companies are doing it therefore we can do it too. We can't have a double standard.

So we cannot have on the one hand companies saying we're doing it because the Chinese Government made us do it and now the very same week the Chinese Government is saying, oh my goodness, we can do it because they are doing it.

And the third thing about the very interesting timing of the press conference that was given by the Chinese Government is this does matter, this hearing does matter. The timing of their press conference it shows clearly that the government is paying attention, the Chinese Government is paying attention. It does matter to them what this hearing concludes. They are watching this closely. And it is very important the kinds of conclusions and this concrete follow-up that this Committee embarks on because you are being watched.

Mr. SMITH OF NEW JERSEY. Thank you.

Let me ask just a few final questions. You have been so gracious with your time. Just a very, very short story.

In the early 1990s I met with Wei Jingsheng in Beijing when he was let out. And then about 2 or 3 weeks after having dinner with me he was rearrested. And then was finally let out because of his deteriorating health. And they let him out in part, we believe, to try to garner Olympics 2000. You know, it was like a token gesture to say to the world, see, we are free, or we are lenient.

I met with the American Chamber of Commerce in Beijing for a breakfast meeting. And after talking about the broad range of human rights abuses in China asked them to meet with Wei. And told them I had just had dinner with him, it was a good 3-hour dinner. We talked about many, many things. And I said, you ought to hear from a dissident, a man who has just come out of the prison. There was no interest whatsoever.

As a matter of fact, when I talked about religious persecution I was told by one member, he goes, well, my secretary goes to church every week. I said, yes, as part of the Catholic Patriotic Association which is under the aegis of the Communist Party. And he did not know that.

So there is this Potemkin village mentality that I find exceedingly disturbing. And all of the human rights groups and people like yourselves continue to bear witness to this and yet it seems to fall on deaf ears. Hopefully today begins a process whereby at least these Internet companies will begin saying what is the consequence when we fork over this information that is on our e-mail server? Where does that person go? Are they tortured? And begin to read some of these documents and become sensitized to these issues.

So that is more of a statement than a question. But let me just ask about, Ms. Liu, you mentioned anti-religious sites. I think it was you who mentioned that you go to the Uyghur, how not to be

a Uyghur, how not to be a Uyghur. And I am wondering if that is a trend.

Because I know the Falun Gong, because I read People's Daily, I have it bookmarked and I go to it virtually every day, and it is rife with anti-Falun Gong tirades, you know, in terms of almost every day. What is, you know, is Google now helping and other search engines to facilitate an anti-Christian, anti-Buddhist, anti-Uyghur? Do you see any evidence of that? You did mention the Uyghurs. And that is something I had not seen other than on People's Daily.

Ms. LIU. Xinjiang Uyghur Autonomous Region we find that there are very stringent controls over religion there. And the Islamic religion that is adopted by many of the ethnic Uyghurs is severely disciplined, discouraged. If Uyghurs are even seen talking to each other about anything remotely religious they are persecuted for it.

I would say, yes, there is religious persecution and, yes, in the Uyghur Autonomous Region it is very serious.

Mr. SMITH OF NEW JERSEY. And the Internet is being used to facilitate that. Yes, sir?

Mr. QIANG. There is a very wide range of the censorship online and offline contents. We often mention Falun Gong, we mentioned Tiananmen massacre. These are absolutely. Taiwan independence. But also those current events for political needs even local governments can issue certain orders to censor the online censorship. There are 14 government ministries, all can issue what is controlled online.

But coming to the Uyghur, that actually belongs to one of the most sensitive information that they watch because they consider the ethnic conflict in the region as a great danger for their control. This point I believe the services such as Radio Free Asia have done a great service to the outer Chinese because that kind of effort people can hear some more information other than the Chinese censor controls.

Mr. SMITH OF NEW JERSEY. Let me conclude, Ms. Hom, you mentioned the follow-up being important. This hearing was several months in the making, in terms of its discussion. We have been working on legislation that will be introduced. I will introduce it. Mr. Payne will be the co-sponsor. And we hopefully will draw a very, very strong bipartisan, and really conservative, moderates and liberals across the spectrum.

It has as its key features, and I will just name a few of them, an office on global Internet freedom. The President would designate each year what would be called Internet restricting countries. And it is not unlike what we did with the trafficking legislation where tier three are countries that are not meeting minimum standards. This would be a country that, you know, would be so branded and then a number of things would flow from that. E-mail servers, and we thank Reporters Without Borders for their insistence on this, you know, time and again, you know, the e-mail server not be located inside of a repressive country where it is, you know, again easily accessible by the secret police.

And we have a number of things dealing with a right to sue for those are the aggrieved party because of this search engine integrity, and on and on.

I would hope as you look at the legislation, and every piece of legislation that I have introduced is always a work in progress from date of introduction, as well as before, give us your best thoughts as to what ought to be in there. And I did ask our friends from the Internet companies to do likewise. We really want absolute transparency in pushing this because at the end of the day we want a free Internet and not people who are then victims because they utilized it in China or anywhere else.

We also point out that there are many other countries where this is a problem. Belarus, Burma, Cuba, Iran, Libya, Nepal, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan and Vietnam. And on Vietnam I would just point out parenthetically and Eleanor Nagy, who is our Director of Policy and I, on the Committee, were in Vietnam in early December. And we met with a number of dissidents including Thich Quang Do and a whole host of other great and courageous men and women. And we found as well there that the Internet is another tool, not as sophisticated apparently, but a tool of repression.

We met with the wife of Dr. Pham Hong Son who got 5 years, and I hope that everybody who may be watching this will realize in Vietnam this individual Dr. Pham Hong Son downloaded from the U.S. Embassy site in Hanoi an essay called "What Is Democracy," and for that he got 5 years in prison and 6 years to follow that of house arrest. His wife met with us for a late dinner just in a hotel. We did it very much in the open so they would not drag her off as well. And sure enough, just a couple of feet away were the bully boys from the secret police standing up and taking pictures with their cell phones, making it very obvious. As one of our witnesses had said, I think, Ms. Liu, you said it earlier that they want to be obvious. Well, they were very obvious. We knew who they were, we took their picture as well.

But it was one of those things where, you know, and she feels very intimidated. And then in all these other countries.

But it seems to me if China continues to get away with it and to do so with impunity and to perfect the art of surveillance, incarceration and torture of those who are democracy minded others will follow suit and perfect and hone their skills. So I mean this is not over yet. We are at a pivot point it seems to me that it could get worse rather than better.

And I think one of you mentioned, I am sorry I don't know, remember who, that the—I think Ms. Hom, that there has been a deterioration of human rights in China. That is contrary to the conventional wisdom of people who say if you just trade, trade, trade somehow a dictatorship will matriculate into a democracy as if by magic. It happens because of the people on the ground. Eastern Europe, Warsaw Pact, U.S.S.R., they became democracies—although we are worried about Russia again—simply because of the people on the ground, the Havels and the Lech Walesas, the Anatoly Sharansky's and so many others who paid penalties to get there. And the penalty of our corporations of standing up is that they may lose some business.

I just would ask you to look at the legislation. The key will be in the follow-up. This is our launching pad, this hearing, to try to

do our level best to make a difference. You already have. And I just am so admiring of the work you do.

If you have anything you would like to close with, any of our distinguished witnesses before we end the hearing? Mr. Wu?

Mr. WU. Congressman, I really want to make a separate suggestion that the Cisco issue is not only like a moral or political consideration, Cisco is violating American law. I think Congress must look into it, and the Government must implement the law. And Cisco really goes too far, okay.

See, this is another document, copyrighted by Cisco, how to train the Chinese police, okay. They knew China very well and the document said China only have 1.6 million policemen and for such a big country, this number of police is not enough. So if you are using our products, our technology then you will have more effective police work. They are working directly with security. It doesn't matter what product you are selling to China, you cooperate with training the police to survey people. You only know about a few people like Shi Tao, and this was because Yahoo! offered IP information that went to court. How many unknown people have been caught by Chinese security because they have Cisco equipment and technology.

Thank you.

Mr. SMITH OF NEW JERSEY. Very important point.

Mr. Wu, if you could just, how many trained secret police are now cyberpolice? Do we have any sense of that? I have heard 30,000, I have heard 35,000.

Mr. WU. Right now there are at least 35,000 Internet police. Maybe Xiao Qiang has more information about it.

Mr. QIANG. Well, there is different reporting. My knowledge is there is no accurate numbers. But what do we know is entire separate division arm of the public security in parallel with fire police or criminal police and political police or traffic police. It is over, spread over 700 Chinese cities and towns, where there is Internet where the Internet police. So the real number I think 30,000 may be underestimation.

Mr. SMITH OF NEW JERSEY. I thank you.

And let me just thank you again. I would ask unanimous consent that a number of submissions for testimony be made a part of the record. [No response.] Without objection, so ordered.

And I would like to thank Eleanor Nagy who is our Chief Director of Public Policy for the Subcommittee, Brad Dayspring, Doug Anderson, Dennis Curry and Lindsey Plumley and Mary Noonan, who have all done yeomen's work to make this hearing as well as this legislation that we will introduce tomorrow a reality.

And again I want to thank you, you have been outstanding. The hearing is adjourned.

[Whereupon, at 5:17 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

INFORMATION ON UNITED STATES IT COMPANIES INVOLVEMENT IN PRC

Yahoo

- According to Amnesty International, on April 27, 2005 Yahoo cooperated with Chinese authorities in events which led to the sentencing of Shi Tao to ten years in prison for sending information about a Communist Party decision through his Yahoo! email account to a website based in the United States. Mr. Shi's appeal was denied on June 2, 2005. The information that led to Mr. Shi's conviction was not demanded by a court order. According to the court transcript of the *Changsha Intermediate People's Court of Hunan Province Criminal Verdict*, evidence presented by the prosecutor that led to the sentencing of Mr. Shi included account-holder information provided by Yahoo! Holdings (Hong Kong) Ltd. Yahoo! has admitted that their subsidiary provided this evidence by correcting the record to state that the information was provided not directly by Yahoo! Holdings (Hong Kong) Ltd. but by Yahoo! China, which is held by Yahoo! Holdings (Hong Kong) Ltd.
- Li Zhi was sentenced on December 10, 2003 to eight years in prison for "inciting subversion." His crime was criticism in online discussion groups and articles of the corruption of local officials. It is believed that Mr. Li was targeted because of his involvement with the China Democratic Party, a political group outlawed in China. A 2004 appeals document released by Li's lawyers revealed that Yahoo Holdings (Hong Kong) Ltd. in 2003 provided Chinese police with information that tied Li to a Yahoo e-mail account as well as messages from that account.
- Reporters Without Borders has reported that since 2002, Yahoo! has agreed to censor the results obtained by the Chinese version of its search engine in accordance with a blacklist provided by the Chinese government. In 2002, Yahoo voluntarily signed a pledge of "self-discipline" promising to follow China's censorship laws. Signatories agreed not to post information that would "jeopardize state security and disrupt social stability."
- Yahoo! reports that it received $30 million in revenue from its operations in China during the first 10 months of 2005. Currently, Yahoo has 21% of the search engine market share in China.Yahoo! started its business venture in China in May of 1998 with Yahoo! China. As of October 24, 2005, Yahoo! entered into a partnership with China's leading e-commerce company, Alibaba.com. As a result, Yahoo! now owns a more than 40 percent economic interest with 35 percent voting rights, making it the largest investor in Alibaba.com.

Microsoft

- In a letter to Microsoft, Amnesty International said that Microsoft's search engine MSN blocks searches under certain key words, including "democracy", "freedom", "human rights", Falun Gong", "June 4", and "demonstration", among others. In China, users of the product Microsoft Spaces are also prohibited from using these and other words on weblogs they create. As a result, websites and webpages dealing with human rights, including those of Amnesty International and other human rights organizations, are inaccessible to internet users in China.
- Those who attempt to search for these words receive an error message announcing "this item contains forbidden speech" reports Human Rights Watch.

- Microsoft reported that it shut down the blog of a Zhao Jing on December 30, 2005. The content of Zhao's blog on MSN Spaces was offensive to the PRC. Mr. Zhao had tried to organize a walk-off of journalists at the *Beijing News*, whose editor was fired for reporting on clashes between Chinese citizens and police in southern China. The blog was hosted on servers based in the United States
- In June 2005, MSN Spaces began removing words like "democracy" and "human rights" from use in Chinese blog titles and postings, according to the Congressional Research Service.
- Microsoft's first office in China was set up in Beijing in 1992. One of Microsoft's main software research laboratories is located in Beijing, which employs over 400 highly skilled engineers.

Google

- Google.com reports that it first struck a deal with China in 2000, when NetEase, China's leading internet technology partner, selected Google as its premier Chinese language-specific search engine and default web search results provider. Under the agreement, Google provided its Chinese language-specific search and underlying global web search engine to complement NetEase's web directory and content channel network.
- On January 25, 2006 Google launched its censored search service google.cn in China. All news and information sources censored in China have been withdrawn by Google from the Chinese version of its news search engine, Google News. Google said it planned to notify users when access had been restricted on certain search terms.
- Google has been collaborating with Chinese censorship of its news service since September 2004.
- Google is also a part-owner of the biggest Chinese search engine, Baidu, which is compliant with government censorship (2.6% share as of January, 2006). The BBC reported that a survey last August revealed Google was losing market share to Beijing-based rival Baidu.com. In 2004, Google had $3.7 million in ad-revenue from China, according to estimates from research firm Shanghai iResearch Co
- Google has said that its e-mail, chat room and blogging services will not be available because of concerns the government could demand users' personal information.

Cisco

- Cisco has profited greatly by providing the Chinese government with the technology necessary to filter internet content through its creation of Policenet, one of the tools the regime uses to control the internet. Cisco's estimated profit from sales to China according to Derek Bambauer of *Legal Affairs* is estimated to be $500 million and holds 60 percent of the Chinese market for routers, switches, and other sophisticated networking gear. The company anticipates that China will soon become its third largest market, just behind the U.S. and Japan.
- According to Harry Wu, Cisco Systems has marketed its Policenet equipment specifically designed to make it easier for the Chinese police to carry out surveillance of electronic communications. Cisco is also suspected of giving Chinese engineers training in how to use its products to censor the Internet. Policenet currently operates in all but one of China's provinces. Policenet connects officials of the Public Security Bureau—a national agency with local branches that handle security, immigration, "social order," and law enforcement—to each other and to electronic records that store a wealth of information on every citizen in China. Along with Policenet, Cisco also produced the watchdog router that prevents Internet users in China from gaining access to banned websites.
- Reporters Without Borders said that Cisco Systems has sold China several thousand routers at more that 16,000 euros each for use in building the regime's surveillance infrastructure.This equipment that was programmed with the help of Cisco engineers allows the Chinese authorities to read data transmitted on the Internet and to spot "subversive" key words. The police are able to identify who visits banned sites and who sends "dangerous" e-mail messages
- In its recent router contract for CN2, Cisco will provide China with its 12000 Series routers, which are equipped with filtering capability typically used to

prevent Internet attacks, but can also be used by PRC authorities to block politically sensitive information according to the Congressional Research Service.

SunMicrosystems

- Researcher Greg Walton wrote that Sun Microsystems is involved in transferring high-tech expertise to the Chinese security apparatus. Working with ChangchunÿsHongda Group, market leaders in fingerprint recognition technology, Sun Microsystems developed a computer network linking all 33 provincial level police bureaus, forming one layer of the Golden Shield, allowing the PSB instant comparison of fingerprints with a nationwide database.

Juniper Networks

- In an effort to assist China with its latest network upgrade Juniper Newtworks secured PRC contracts for such work. Juniper Networks, Inc., announced in 2004 that it had been awarded the largest share of the contract for China Telecom's next-generation backbone network. China Telecom, the country's leading telecommunications provider, selected Juniper Networks routing platforms exclusively for its national core backbone and eight South China provincial backbone networks.
- Juniper Networks has announced that the China Next Generation Internet (CNGI) IPv6 project will be powered by Juniper's M- and T-series routing platforms. IPV6 will create an alternate to the 30-year-old IPv4 protocol which forms the backbone of the internet today.

STATEMENT SUBMITTED FOR THE RECORD BY MR. DAVID JACKSON, DIRECTOR, VOICE OF AMERICA

HOW CHINA BLOCKS THE VOICE OF AMERICA

The Voice of America broadcasts news and information 18 hours a day into China: 12 hours in Mandarin, 4 hours in Tibetan, and 2 hours in Cantonese. Two of VOA's 12 hours per day of broadcasting in Mandarin are television programs that include news, discussions of U.S. policy, American democracy, health, science, business, and programs that introduce and explain developments in America, China, and the rest of the world. These radio and television programs also include live call-in shows, discussions of human rights, interviews of members of Congress and other U.S. Government officials that discuss U.S. policy, as well as English-language teaching and audience mail shows. The television and radio programs are available on the Internet in streaming audio and video as well as in news scripts.

In addition, VOA maintains extensive websites in the Chinese and Tibetan languages. The Mandarin site, for example, provides updated news that is picked up and redistributed (sometimes without the VOA byline) an average of four times a day by newspapers, magazines, blogs, chatrooms and websites inside China. VOA's Chinese language reports are also regularly included in China-bound email news services by such popular overseas Chinese portals as *Chinesenewsnet.com* and *Boxun.com*.

Despite—or because of—this popularity, the PRC does everything it can to block VOA's broadcasts in clear violation of accepted international rules and regulations followed by almost all other nations, and that they have agreed to adopt as well, and it is doing the same with VOA's Internet sites. The Internet is becoming a critical component in distributing program materials to those countries that are—or are becoming—"wired," and China has the largest number of Internet users in the world after the United States. The number of Internet users in China was estimated at 111 million, according to the China Internet Network Information Center, and is rising at a faster rate than in any large country in the world. Internet delivery will become increasingly more important to the future of U.S. international broadcasting in China.

VOA's website has been blocked in China since 1997; the ban has been lifted only occasionally, such as during a visit by a U.S. president. Chinese jamming of VOA radio is equally pervasive. The radio jamming usually consists of repeated loops of the sounds of Chinese drums or opera music. Two years ago, China installed "ground jamming" transmitters on hilltops around the Tibetan capital of Lhasa.

The year 2005 saw a sharp deterioration in China's attitude toward VOA. Scores of radio and television stations inside China that carry VOA programming—after stripping off all identifiers—were regularly harassed by messages from Beijing ordering them to beware of the impact of VOA's programming. In 2004, two stations almost lost their broadcasting licenses after airing VOA reports on the U.S. presi-

dential elections. In 2005, China refused to allow VOA to participate in an event inside China that Beijing organized on behalf of the Asian Broadcasting Union, even though VOA is a dues-paying member of that organization. Last year, China also began banning VOA from renting booths under the VOA name at TV and radio trade fairs in Shanghai, Beijing, and Chengdu.

China continues to block VOA programming regardless of the program content. For this year's Chinese New Year, a provincial radio station in China requested that VOA organize a joint-broadcast on how Chinese from that province were celebrating the New Year in the United States. VOA and the Chinese station planned an ambitious and entertaining joint program, but six hours before the planned broadcast, Beijing ordered the provincial station to cancel the program.

In early 2005, a high ranking official in Beijing called VOA "subversive." What does China have to fear from VOA? Quite a lot, in their view. VOA provides news about China that has not been censored. VOA offers an unbiased and comprehensive perspective on world events far from China's borders. But most of all, VOA offers an objective and informative view of and from the United States and the American people. China would much prefer to have its official media cultivate and manipulate perceptions of the United States. While the Chinese government uses the Internet as a driver for knowledge transfer and business development, it ruthlessly suppresses any attempt to use the Internet for issues as diverse as Tibetan freedom, corruption, environmental pollution, pro-democracy movements, or religious groups such as the Falun Gong.

Congressionally-funded enhancements have helped VOA to develop a variety of services designed to outflank China's firewall. The Broadcasting Board of Governors (BBG) established a special unit to devote technical resources to this problem, consulting with industry and government experts on what works and what doesn't in terms of getting information into China.

VOA now emails daily news bulletins to millions of subscribers inside China. VOA also uses a series of newly developed, imaginative, and creative methods to let Internet users inside China access the broad array of information on VOA's official websites. In each of the emails, we include information on several different "proxy" sites that we have developed to stand in for forbidden sites. Even though VOA may be blocked, we can distribute alternative site names to viewers through which they can establish a connection to an unblocked site—and access to VOA, Radio Free Asia (RFA), or nearly any other site on the Internet. We have received thousands of unique visitors every day on each of the proxy sites, with most of the traffic accessing VOA's Chinese language news and information sites.

VOA is using the Internet to deliver content in a number of innovative ways. Audio streams are offered in Windows, Real and MP3 files. RSS feeds are available for most languages, which allow other content providers and blog sites to syndicate our content. We're offering a growing number of podcasts, including the popular Special English version. We have also begun testing a mobile web page for accessing VOA in multiple languages with a cell phone or PDA. Soon we plan to offer on-line chat that will allow Internet users to participate in discussions with experts in multiple languages using Instant Messaging and email.

Our efforts to combat broadcast jamming and Internet blockage are paying off. VOA's broadcasts to China have consistently enjoyed the largest audience share among international broadcasters, according to audience surveys conducted by Intermedia Research, Inc. VOA's regular audience numbers more than 10 million. In China, people listen mostly to our shortwave radio broadcasts, despite severe jamming. Television also attracts viewers, especially in Tibet, where VOA is the only non-censored source of television news. Tibetans who traveled from inside Tibet to the Dalai Lama's January, 2006 Kalachakra in India told Intermedia's researchers that they regularly tape VOA's TV broadcasts and then distribute copies to their friends inside Tibet.

VOA also enjoys the highest awareness rating of all international broadcasters, with more than 60 million Mandarin-speakers recognizing VOA's brand name. These figures represent the tip of the iceberg for VOA, because Chinese inside China generally decline to admit that they listen to foreign broadcasts for news since their government discourages it.

Despite China's regulations outlawing "counterrevolutionary" correspondence with "enemy" broadcasters, the Voice of America receives thousands of letters and emails every month proving that many Chinese are still eager for uncensored information. Recent comments from VOA's audience in China clearly document both Beijing's jamming and the determined efforts of the Chinese people to gain access to VOA's broadcast information and Internet sites:

From email:

I am one of your loyal listeners who lives in Shenzhen. I have been listening to your radio broadcasting for 6 years! Recently I switched to your on-line broadcasting and the results are very good. However, your web site is often blocked by the Chinese authorities and cannot be accessed. Sometimes even proxy addresses are blocked, too and that frustrated me a lot!

From email:

Very glad to receive your reply. I am now subscribing to your email news and "Popular American." Although I can often receive your email, I cannot click open your web page. But I could open your web pages during the Spring Festival. Occasionally during holidays, your web page can be accessed and "Popular American" can be read. This may be a problem on the Chinese side! As a matter of fact, (your) bilingual news is quite important to me. But I have no way out! The proxy addresses you provide work for your web site. But your site is either English or Chinese, not so as convenient as your (bilingual) email news. But thanks anyway!

From email:

I'm a Chinese student and I like VOA! But in China we can not visit your website because of our political reasons. So can you send me frequencies of VOA including Special English? Thank you very much!

From email:

I have been using the following [proxy] addresses to visit your web site. But now they have all been blocked . . . Please tell me what to do and what [proxy] addresses I should use to enter your site? Thanks! I am very anxious.)

From email:

Every time I try to open your web site, I always get "Error display page," whereas such (error messages) never or rarely occur on other web sites. The "Uncut News" page is not accessible.

From Yunnan:

The reception of VOA Chinese programs is horrible, almost completely contained by China Central Radio. Often times it is impossible to listen to. I suggest VOA set up relay station in neighboring countries such as Pakistan, and also broadcast from a few more frequencies.

From email:

I started to listen to your programs since I was 12 and now I am 25 years old. I was then guided by my father. Your programs accompanied me to get through my schools years. My father also wrote to you many times before, although most of the letter he wrote to you disappeared forever. The very rare responses would always make us very excited. It's more convenient now that we have the internet. I've already subscribed to your email news for more than a year. I hope you can provide me some more proxy addresses.

The BBG has documented Chinese interference in VOA and Radio Free Asia broadcasts, and complaints have been filed through the Federal Communications Commission to the International Telecommunications Union in Geneva, but with no success, as Beijing claims the frequencies belong to them. The Broadcasting Board of Governors and the State Department have complained directly to the PRC Foreign Ministry, State Council and State Administration for Radio Film and Television about blocking VOA's Internet sites and radio signals. Despite objections from the BBG and the U.S. Embassy in Beijing, China continues to intentionally jam radio transmissions and to block our web sites while aggressively promoting Chinese government television and radio programming in the United States.

The PRC government's blocking of VOA web sites inhibits the capability of Chinese to watch VOA's television news programs in streaming video as well as to listen to VOA radio news in streaming audio and to read VOA's Web-based news scripts and English-language lessons. Such censorship also blocks or inhibits Chinese from participating in VOA programs through email and Internet traffic. VOA's response has been to deliver daily news emails and proxy information to more than 53 million subscribers inside China every week. The Chinese government attempts to block these emails but is largely unsuccessful because of efforts by the BBG's Engineering Directorate to utilize the latest technology to avoid the censorship.

Recently, it has been reported that several U.S. companies have developed ways to comply with filtering/censoring requests by the Chinese government. Now there are explicit differences in the search results returned by Google, depending on

whether one accesses the U.S. or Chinese Google server. Shortly after Google agreed to filter results in line with PRC orthodoxy, the results of a Google image search for Tiananmen Square showed that when the .com site is accessed, one finds images of soldiers, protesters, and general scenes of conflict, highlighted by the famous photo of the young man facing down the tanks. But if one does the same search on the .cn site (for Chinese), one receives a nice photo of couples and young families having picnics on the square. The difference between the two sites is disturbing and points out the difference between unbiased news and information and censorship, enabled by an American company and technology.

In fulfilling VOA's Charter and communicating directly with audiences around the world, VOA believes that greater understanding between peoples can help lead to peaceful resolution of our differences and an appreciation of our similarities. China's attempt to block the free flow of news and information and informed discussion of issues is hindering rather than enhancing that understanding.

UYGHUR PRESS RELEASE

CHINA BANS OFFICIALS, STATE EMPLOYEES, CHILDREN FROM MOSQUES

2006.02.06

HONG KONG—Chinese authorities have tightened curbs on minority Muslims in the northwestern region of Xinjiang, banning any government officials, state employees, Party members, and in some cases women from entering mosques.

A photo sent to RFA's Uyghur service shows a sign above the gate of a mosque in the poorer southern part of the Xinjiang Uyghur Autonomous Region, forbidding Muslims to attend for worship—as they are supposed to do five times a day.

"The following people are prohibited from entering the mosque and conducting religious activities," reads the sign, written in the language of the main Muslim ethnic group, Uyghur, which uses the Arabic alphabet.

"1) Communist Party members and Communist Youth members. 2) State employees, workers, and retirees. 3) Youths under the age of 18," it says. Categories four and five are local government employees and women, the first time such gender restrictions have been alluded to.

An imam, or religious teacher, at the Heitkar Mosque in Kashgar, the biggest mosque in the region, confirmed some of the restrictions, although his initial reply seemed aimed at avoiding direct criticism of Chinese Communist Party policy.

Imam's awkward responses

Asked who was allowed to worship in Xinjiang's mosques, the imam replied: "Everybody. Every Islamic believer is allowed."

But confronted with restrictions in other mosques, he confirmed that such rules did exist at Heitkar, too.

"Same. It is same here in our Heitkar mosque too. Our policies are all same," the imam said.

Several Uyghur Muslims confirmed to RFA that those who fell under certain categories were unable to attend mosque for daily prayers, or even for major festivals such as Eid al-Fitr at the end of the fasting month of Ramadan, or Eid al-Adha at which sheep and goats are sacrificed to recall the sparing of Abraham's son Ismail.

"There are signs on the mosque walls stating that people under 18 are prohibited. And they talk about that every village meeting," a farmer from the countryside near Kashgar said.

Dissent restricted

"Though the Chinese government's religious policy is causing strong discontentment, people are still showing forbearance towards the Chinese government's unfair policies against Uyghur Muslims, since even dissenting opinions are restricted," he said.

The farmer also confirmed that government officials kept tight guard over mosques, noting who came and left and issuing fines of 1,000–5,000 yuan (U.S.$124–620) to those who broke the ban.

"From small units of countryside headmans to the students, they are all banned from mosque . . . Even for the Eid prayer, they are not allowed," he said.

He cited the case of a schoolteacher jailed for two years and fired after 20 years' service for persisting in her religious faith.

"If an imam does not do what the government says, the government will appoint a new one who will," he told RFA reporter Guljekre.

No bonus for festivals

Besides Uyghur Muslims, Kazakh and Chinese (Hui) Muslims were affected by Beijing's religious policies in Xinjiang.

"The unity of all nationalities is going well," said the Hui Muslim man. "But there is not any aid or bonus when we celebrate festivals. When Chinese people celebrate they get bonuses. So we should also get something when we minorities celebrate festivals. But there is nothing."

In a 2005 report, Human Rights Watch and Human Rights in China argued that Beijing is sharply tightening religious curbs on Uyghurs.

"Uyghurs are seen by Beijing as an ethno-nationalist threat to the Chinese state," Sharon Hom, executive director of Human Rights in China, said. "As Islam is perceived as underpinning Uyghur ethnic identity, China has taken draconian steps to smother Islam as a means of subordinating Uyghur nationalist sentiment."

Original reporting in Uyghur by Guljekre. RFA Uyghur service director: Dolkun Kamberi. Written for the Web in English by Luisetta Mudie. Edited by Sarah Jackson-Han.

UYGHUR OFFICIALS SAY FAMILY PLANNING, RELIGIOUS STRIFE BEHIND DEATH OF COMMUNIST OFFICIAL

2005.07.26

HONG KONG—Two Uyghur officials in northwest China have said forced abortion and conflict over religious issues lay behind the killing of a Communist Party village official earlier this year, which led to the trial and execution of two Uyghur young men for murder, religious extremism and separatism.

Sulayman Obul, 30, and Abdurehim Husseyin, 19, were executed in April after being convicted of murdering Matsalihan Ahmet, their local village Party secretary in Karkash County, around 2,000 kms to the south-west of Urumchi, local media reported.

But while the Urumchi-based *Modern Xinjiang* newspaper recorded Matsalihan's death as an honorable one, it did not report allegations that the late village Party chief had opposed the building of a new mosque, or that the slain man had tried to force Sulayman Obul's wife to abort the baby she was carrying.

"The two people now . . . we gave them the death penalty and they lost their political freedom and status and the penalty has been executed," Karkash County government official Tursun Niyaz confirmed to RFA's Uyghur service.

Religious tensions abound

"One of them was the Imam's son and other one was the preacher's son. One of them, Sulayman, was the son of the Imam of the Ulughata mosque," he said.

Imams and other religious educators are frequently targeted by Beijing, which fears an Islamist uprising against Chinese rule, which is deeply unpopular in the region.

He said the two men were found guilty of intentional murder, religious extremism, and separatism by the Intermediate People's Court in Hotan, a city 23 kms southeast of Karkash.

Current village Party secretary Erkin [one name correct] confirmed that forced abortion was at issue between Sulayman and Matsalihan prior to the killing.

"It is true, once he, Matsalihan, had asked Sulayman Obul to have his wife abort their child during a family planning meeting," Erkin said.

"He criticized him, saying his wife was pregnant year after year," he added.

Dead official 'loyal' to Party

"The family planning rules say a family must wait for three years before they can have permission," Erkin said. "They cannot have children every year. They can have three children, but it must be done during nine years . . . but they must be only one every three years."

Asked whether it was against the religious beliefs of Muslims, for whom abortion is a sin, Erkin replied: "Right! But there are plenty of things like that. If the woman is pregnant before the end of the third year, it happens everywhere," he told RFA.

Asked about his understanding of the motive behind the killing, Tursun Niyaz said: "Well, they are, er [audible sigh], we may call them religious extremists. In the Uyghur language, we might call them hot-blooded or paranoid-people who do not know what they are doing."

"This killing was an accident," he said, in contrast to the court verdict of intentional homicide.

"[Matsalihan Ahmet] was the Party leader of the village. He was the only loyal representative of the party in the village. Second of all, he was continuously fighting

against illegal religious activities and separatism and religious extremism," he added.

And replying to allegations by local residents that Matsalihan Ahmet had blocked the buiding of a new mosque for the village, Tursun Niyaz said:

"They had planned to attack the government officials who enforce [Chinese] law, because the religious extremists believe that the officials are strict with religious practices and with family planning rules."

"It is not about opposing building mosques because there are mosques here and they had built mosques with help of Matsalihan," he told RFA.

Original reporting by RFA's Uyghur service. Service director: Dolkun Kamberi. Produced for the Web in English by Luisetta Mudie.

CHINA STEPS UP RELIGIOUS CONTROLS OVER MUSLIM UYGHURS

2004.11.17

WASHINGTON—Top Chinese officials in the northwestern Muslim region of Xinjiang have called for an intensification of 'ideological work' among the country's ethnic Uyghur university students. Meanwhile, RFA has learned that local officials were ordered once more this year to report anyone fasting during the month of Ramadan.

"We have an agreement with the Chinese government that I am responsible for preventing students from fasting during Ramadan," an official from a county-level religious affairs committee in the south of the region told RFA's Uyghur service.

"If I find out that any of them have been fasting I have to report it," said the official, who declined to be identified.

Beijing says there are more than 20 million Muslims in China, who have access to 40,000 Islamic places of worship, and more than 45,000 imams, or religious teachers.

But it imposes harsh restrictions on the Turkic-speaking Uyghur population, who are deeply discontented with Beijing's rule, in the fear that Islamic activities will fuel separatist fervor there.

In most Islamic societies restaurants remain closed from dawn to dusk during the month of Ramadan, when the majority of the adult population is fasting. Not in Xinjiang, the official said.

Move aimed at 'stability'

"I am responsible for making sure that the restaurants stay open as normal. I have to write a report every day for the officials higher up about the situation and also I have two people on duty at night to pass on information and report to higher up," he said.

Exiled Uyghurs say it is a frequent occurrence for Uyghur employees to be taken out for big lunches by their Chinese employers during Ramadan.

The Lop county official reported similar actions. "In our town, fasting is not allowed," he said. "At about 4:30 p.m., before the kids leave high school, they will give them candy to eat."

Under China's "10 No's" policy governing Xinjiang, young people under 18 years old are forbidden to attend mosque, or to take part in religious activities.

Beijing's "Strike Hard" campaign against Uyghur separatists, who would like to see an independent Uyghur republic of East Turkestan, intensified following the Sept. 11 attacks in the United States.

The campaign has used the political momentum from President George W. Bush's war on terror to crack down on violent and non-violent advocates of change alike.

The practice of Islam in Xinjiang has become increasingly politicized as a result of this ideological linkage with separatism and terror.

In a recent speech to regional officials, deputy regional Party secretary Nu'er Baikeli called for an intensification of the Communist Party's ideological education program in Xinjiang's universities, suggesting that a ban on religious activities already in place at the region's top Xinjiang University would soon be extended throughout the higher education system.

Censorship of Friday sermons

"We need to widen the territory for our propaganda work . . . into the classroom, study groups and community activities," he told a conference on ideological work in Xinjiang.

"We must step up the management of media propaganda and publications at every level," he said. "We must not give any opportunity for wrong thinking to be disseminated."

The Lop county official confirmed reports from overseas groups that the Chinese authorities were continuing a program of heavy religious control and censorship in Xinjiang.

"No one other than government appointed imams or mullahs is allowed to give religious instruction. Also you can't say anything that damages the relationship between ethnic groups in China [criticize Beijing]," he told RFA.

"You are only allowed to do religious activities in officially recognized mosques. The expounding on the Koran in Friday sermons is not allowed to take longer than half an hour."

"Before Friday prayers, a higher-up official will come and ask if there are any problems from the previous week or anything that we can't handle and need help with. They also have special interpretation guidelines for Friday's religious guidelines. Interpreters of the Koran cannot have their own interpretations," the official said.

Uyghurs constitute a distinct, Turkic-speaking, Muslim minority in northwestern China and Central Asia. They have twice declared a short-lived East Turkestan Republic in Xinjiang in the 1930s and the late 1940s but have remained under Beijing's control since 1949.

According to a Chinese Government white paper, in 1998 Xinjiang comprised 8 million Uyghurs, 2.5 million other ethnic minorities, and 6.4 million Han Chinese—up from 300,000 Han in 1949. Most Uyghurs are poor farmers, and at least 25 percent are illiterate.

Uyghur Service Listener Letters

"Yesterday when I heard the RFA Uyghur service report, listening to the warm voice of Rebiya Kadeer, I don't know why but I started to cry. I am a tough-hearted person, and I never cry easily, but I cried. I believe that when softer-hearted people listen to her voice—when they heard her say, 'I am free, I can talk to anybody I want, I can see anyone I want,' they will also cry, and they will cry loudly."—Listener from the Xinjiang Uyghur Autonomous Region

"RFA broadcasts, like an educator, have brightened our heart . . . They have opened our eyes. China always wants to keep the Uyghurs ignorant of the world. But now we understand democracy, human rights, and freedom. RFA broadcasting means more than food, drink, and air to us, because it gives us hope and inspiration. We hope RFA increases broadcasting time in the Uyghur language."—RFA Uyghur service listener

"The [RFA] programs speak to my heart . . . The world must hear what is going on here."—RFA Uyghur service listener

"There are about two million Uyghurs living in the republics of Kazakhstan, Uzbekistan, Kyrgyzstan, and Tajikistan . . . Since no reliable Uyghur-language media exist in the region, most Uyghurs listen to RFA Uyghur programming. RFA-Uyghur plays a great role in our daily life and education."—Uyghur listener in Tashkent

---

STATEMENT SUBMITTED FOR THE RECORD BY MR. TOM MALINOWSKI, WASHINGTON ADVOCACY DIRECTOR, HUMAN RIGHTS WATCH

Mr. Chairman, thank you for convening this hearing and for asking me and Human Rights Watch to submit testimony.

First, the Internet clearly has the potential to be a liberating force in repressive societies. In China, millions of people have used the Internet to discuss previously taboo topics, to criticize their leaders in ways that would have been impossible just a few years before, and to obtain information their government would rather they not have. That is why the Chinese government is so worried about this medium. That is why it is cracking down.

Second, the Internet gets its liberating potential from two basic qualities—it provides free and instantaneous access to information and ideas, and it allows people to communicate anonymously. But as China is showing, these qualities can be taken away. And once you take away users' anonymity and censor, for political ends, the content they can see, the Internet is no longer a liberating medium. In fact, it can become a tool of repression.

Therefore, it is not enough for Internet companies to argue that their mere presence in countries like China will lead to political openness. It is illogical for companies to say they are expanding the boundaries of freedom in China if they strip their product of the very qualities that make it a force for greater freedom. These companies must protect the integrity of the product they are providing, or that product

will no longer be the Internet as we know it, and will no longer have the impact on society we all wish to see.

Third, the stakes here are much greater than the future of freedom in China. China is already exporting technology for monitoring the Internet to other repressive governments—Zimbabwe, for example. And such governments in every part of the world are now watching to see if China can bend Internet providers to its will. If China succeeds, other countries will insist on the same degree of compliance, and the companies will have no standing to refuse them. We will have two Internets, one for open societies, and one for closed societies. The whole vision of a world wide web, which breaks down barriers and empowers people to shape their destiny, will be gone. Instead, in the 21st Century, we will have a virtual Iron Curtain dividing the democratic and undemocratic worlds.

WHAT IS HAPPENING IN CHINA?

Internet censorship within China is not a stand-alone policy. It is part of an overall strategy to limit the flow of information within China to what the leadership wants China's citizens to know about their own country and about the world.

Most recently, on January 25, 2006, when mainland authorities shut down the outspoken Bingdian Weekly, authorities succinctly articulated China's approach to information control. A notice of the closure by the Publicity Department of the Chinese Communist Party Central Committee criticized the editor of Bingdian and senior staff at China Youth Daily, its parent publication, for "articles incompatible with the mainstream ideology." Although no particular articles were cited in the notice, earlier criticism had been directed at the weekly's coverage of stories questioning textbook interpretations of sensitive historical events, one going back over one hundred years, another some sixty years.

As the number of Internet users in China has skyrocketed, from 22.5 million (or 1.7 percent of the population) in 2000, to 111 million (or some 8 percent of the population) at the end of 2005, as the diversity of information available through the Internet has mushroomed, and as users have developed expertise in accessing it, the Chinese leadership has devoted extraordinary resources to erecting its Great Firewall.

Even before the recent news about Google censoring its search engine, Internet users already had to contend with a long list of censorship measures including:

- a sophisticated filtering system;
- the banning of unregistered personal domestic websites;
- the September 2005 "Rules on the Administration of Internet News Information Services," which prohibited the distribution of uncensored news stories or commentary through Internet portals, e-mail or SMS, in the interest of "serving socialism," upholding the interests of the State," and "correctly guiding public opinion."
- limits on who could access university Internet message boards;
- the tracking of Internet café users through real-name registration and use of ID numbers;
- blocked websites; and
- the threat of imprisonment for those engaged in dissident speech on the Internet.

But one lesson of China's experience with the Internet is that repressive governments cannot exercise full control over this medium without the willing cooperation of the private sector companies that are leaders in the industry. Bill Clinton had a point when he said that controlling the Internet was like trying to "nail jello to the wall." It just isn't possible—unless you persuade the companies that make jello to change their recipe. And that's what China has been doing.

China sought and received the cooperation of global Internet companies in limiting access to information. In mid-2002, Yahoo! voluntarily signed China's "Public Pledge on Self-discipline for the Chinese Internet Industry." Signing the vaguely worded pledge, sponsored by the government-affiliated Internet Society of China, required that Yahoo! "[r]efrain from producing, posting or disseminating harmful information that may jeopardize state security and disrupt social stability, contravene laws and regulations and spread superstition and obscenity," that it "monitor the information publicized by users on websites according to law and remove the harmful information promptly," and "[r]efrain from establishing links to Web sites that contain harmful information so as to ensure that the content of network information is lawful and healthy." Definitions of key terms were not provided.

Human Rights Watch warned at the time that Yahoo! was in danger of becoming an "information gatekeeper." We tried to persuade Yahoo! that it should bring industry leaders together to resist Chinese blandishments and to remain information gateways. Nothing came of the initiative. Rather, during the past three-and-a-half years, as competition among global Internet companies sharpened, China was able to capitalize on Yahoo's decision to sign on to censorship.

In 2005, Yahoo! provided information that helped Chinese authorities identify Shi Tao, a Chinese journalist, who allegedly "leaked state secrets abroad." He was sentenced to a ten-year prison term in April 2005; the "secret" he allegedly leaked consisted of information about government guidelines for reporting on the June 2004 fifteenth anniversary commemoration of the Tiananmen massacre.

In May 2005, Microsoft's new joint-venture portal users found they could not use the Chinese words for democracy, freedom, human rights, or demonstration to mark personal websites created through MSN Spaces, a free online blog service. The returned error message announced, "this item contains forbidden speech." MSN Spaces is operated by Shanghai MSN Network Communications Technology, in which Microsoft owns a 50 percent stake.

Google reportedly resisted the Chinese government initially, but in November 2004 it began to provide an abridged Chinese service of Google News, using some 1,000 news sites, but excluding from its list of links those from publications the Chinese government found objectionable, such as the Voice of America.

In August 2005, Google partnered with Baidu, another Chinese giant, but it continued to lose market share. Finally on January 24, 2006, Google announced it had installed a server within China to speed service and increase its competitiveness within the Chinese market. It also announced that it would censor certain search results on its search engine that the government finds objectionable, such as those relating to human rights. Google said that it would tell users that the information was being censored, but did not contest the underlying censorship. The company has so far said that it won't provide G-mail or other services that might cause it to run into a Yahoo!-type situation. However, given the compromises Google has already made, the huge market pressure on companies to go into China, and the lack of any laws prohibiting companies from working hand in glove with the Chinese police state, there is no reason to believe that it will permanently refuse to offer those services in China.

HOW DO THE COMPANIES JUSTIFY THEIR ACTIONS?

The Internet companies have made several arguments to defend their compromises in China. I would like to address a few of them, Mr. Chairman.

The first, and most common argument is: "Internet users in countries like China will be better off if American companies are there than if they have to leave." As I've already suggested, that argument is unconvincing if Internet companies censor their content and cooperate with efforts to persecute dissidents in ways that make them indistinguishable from local Internet providers. I hope we can agree on a simple principle: Yes, we want American or other Western companies to play a leading role in developing the Internet in China and other closed societies, but only if their standards with respect to free expression remain significantly higher than local companies in those countries.

A second common argument is: We have to follow Chinese law if we do business in China."

In fact, it's not always clear if the companies are following written law, or just submitting voluntarily to political demands from Chinese leaders—Yahoo, for example, began censoring content after signing a *voluntary* pledge on "self-discipline" in the Internet Industry.

Moreover, the law on this question isn't straightforward. Chinese domestic law forbids dissident speech. But China is also a signatory to the International Covenant on Civil and Political Rights (ICCPR), and is thus obliged to uphold the principles embodied in that document. Censoring information flouts the ICCPR's article 19, which states in part that, "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print . . ." In helping the Chinese government enforce its domestic rules, the Internet companies are also complicit in a clear violation of international law.

That should be reason enough for these companies to challenge the Chinese government when it imposes these dictates—to use the emerging Chinese legal system to fight the Chinese government's rules, to lobby Chinese government officials to relax them, to ask the U.S. and other governments to intervene on their behalf. But as far as we know, the companies have not challenged Chinese rules at all. In the

past, they have suggested that their only choices are either to comply with whatever arbitrary dictates they get from the Chinese state, or to leave China tomorrow. I think that's a false choice.

Of course, when these same companies have been threatened with government restrictions on content and privacy in the United States and Europe, they have not been timid about fighting back. As we all know, Google has refused a U.S. request to turn over information about user searches. Internet companies have strongly opposed a proposed European Union law over content. And good for them. I would just like them to be as brave in dealing with dictatorships as they are in dealing with democracies.

Mr. Chairman, if you or other members of Congress introduce legislation regulating what Internet companies can do in places like China, lobbyists from Yahoo!, Google and Microsoft may well be in your offices using every means of persuasion at their disposal to persuade you to change your mind. And that is their right. But if so, I hope you will ask them why they are making greater efforts to lobby the U.S. government in *defense of censorship* than they ever made to lobby the Chinese government in opposition to censorship.

Of course, changing the Chinese government's policies will be hard. The Companies make a fair point when they say, as Yahoo and Microsoft did in a recent joint statement, that "acting alone, our leverage and ability to influence government policies in various countries severely limited." The companies are also right that the U.S. government should bear some of the burden of dealing with this problem. But if companies do put up a united front and are supported by the U.S. government, they will be in a very strong position. In 1999, for example, technology companies stood up to the Chinese government when it tried to clamp down on the commercial use of cryptography to maintain the confidentiality of corporate communications. Coordinated efforts by various companies and trade agencies forced the Chinese government to drop its demand that encryption codes be turned over.

If such concerted action does not work, then, and only then, will we face the question of whether these companies should stay in China. If we reach that point, I would argue that there are moral lines companies should not cross, even if it means they cannot do business there. No company should ever, under any circumstances, turn over the name of a political dissident to a repressive state. And no company with a stake in the free flow of information should censor information to satisfy the political dictates of a dictatorship.

At some point, a moral bottom line must take precedence.

But the key point is, we're not there yet, because a concerted effort that would make it possible for companies to keep doing business while upholding their principles has not yet been made.

A third argument made by some companies is that censorship is acceptable if Chinese internet users are honestly told what is happening. This is the argument that Google is making, because the Chinese Google site includes a disclaimer at the bottom informing users that some information is being censored.

But is Google really being honest and open about what it is doing? Google is not disclosing crucial information—it is not saying how its censorship system works. It is not telling users what material—what sites, words, and ideas—the Chinese government is telling it to block (or what it is censoring pursuant to any internal policies designed to appease China). I urge the Committee to ask companies to provide this information to the Congress—and to their users.

Perhaps Google is embarrassed to admit that for such a system to work, the company will have to maintain a close and ongoing relationship with the Chinese security apparatus. This is because it will not be enough for the Chinese government to give Google a list of forbidden web sites and search terms just once. If that were the case and our Human Rights Watch site, for example, were excluded from Google search results in China, we could simply set up a mirror site that is not excluded. So it's safe to assume that the Chinese security services will be constantly updating and adding to the list of forbidden sites and terms it requires Google to block—or that they expect Google actively to police its own site, censoring any new information that might displease the Chinese government.

And down the road, I would expect the Chinese government to demand that Google take down even the small disclaimer it currently places on its site. After making far bigger compromises and establishing a close working relationship with the Chinese state, will Google say no to that? And what if the Chinese government then asks Google to take a step further, and turn over the individualized search records of its users? The compromises these companies have made and the relationships they are forging, none of which are transparent, create a very slippery slope.

A fourth argument that companies, including Google, make is that the sites they remove from their search engine results are in any case blocked by the Chinese gov-

ernment, and thus that their Chinese users are not being denied anything to which they previously had access. But this is not entirely true. If you punch in the words "human rights" on Google, you will find links to literally millions of websites, from the home pages of NGOs, to government sites, to newspapers, universities, and blogs in scores of countries around the world. If Google filters by keyword as well as by web addresses, it may filter out web pages that would have escaped a site-block by the Chinese authorities.

Moreover, technologically savvy Internet users in China do have ways of getting around government restrictions on specific Internet sites. But if their search engine is censored, they may never learn that a particular site even exists, and the odds they can overcome the Great Firewall go down considerably. In this way, Google is doing the Chinese government a great favor—something that government could not have done for itself.

A final argument American companies make is that if they don't enter the China market, someone else will and the results will be the same. That is the same argument some companies made in opposing legislation that forbade them bribing foreign officials—"if we don't do it, someone else will." But the Congress didn't buy it. Moreover, the U.S. government then got together with its partners in the industrialized world (through the OECD) and negotiated a global compact against bribery to which dozens of countries now subscribe. There is no reason why the same could not be done here.

Moreover, I'm not so sure that if U.S. companies were to stay out of China (a step that, once again, I do not think will even be necessary), others would just fill the vacuum. Yes, there are local internet providers in China. (Interestingly, the Chinese companies may not even always be as restrictive as the U.S. providers now are! For example, if you type "Radio Free Asia" in Google.cn, there is no link on the first three pages to an RFA website. But if you type it in www.zhongsou.com, a domestic Chinese search engine, the first link is a direct link to Radio Free Europe/Radio Liberty—www.rferl.org).

But let's be realistic—the major American companies are the giants in this industry. When you want to look for information on the Internet, you "Google" it. When you want to manipulate it, you do it on Windows. These companies compete with each other, but they do not have major external competitors. They have enormous bargaining power with any government that wants to be part of the information age. They simply haven't tried to use that power collectively with the Chinese government, because it has been more convenient to cut individual deals and comply with whatever rules Beijing imposes.

WHAT SHOULD THE CONGRESS DO?

The ideal solution to this problem would be a concerted, collective effort by the Internet companies to stand up to Chinese pressure. Yahoo and Microsoft have suggested that they want to find, in their words, "better ways of protecting the interests of all users of our services" and that they are "actively exploring potential approaches to guide the practices of our industry." Human Rights Watch would welcome such an effort and be happy to work with the companies to make it meaningful.

At the same time, the pressure these companies are facing from the Chinese government should be matched by pressure from democratic governments, starting with the United States. The Internet companies natural reaction may be to resist regulation. But I think the companies should welcome efforts by the Congress and the administration to set minimal standards of conduct in this area. Binding standards would free companies from the burden of having to decide, on a case by case basis, how to respond to demands from dictatorships, and make U.S. law and the U.S. government their ally when they are faced with unreasonable and unethical demands.

To begin with, Congress should pass legislation akin to the Foreign Corrupt Practices Act that would forbid U.S. companies from turning over names or other information that would identify specific individuals to foreign governments, when that information is sought to regulate or punish free expression that is protected by international law (i.e., political speech). There needs to be a clear bottom line here. Ratting out dissidents to dictatorships is repugnant behavior. No American company should ever, under any circumstances, feel that such a thing can be justified. It should be absolutely prohibited by U.S. law.

Again, the companies should welcome this kind of prohibition. Cases like that of Shi Tao badly hurt their image and undermine the trust of their customers. And if the rules don't change, it is inevitable that there will be many, many more such cases in the future. The only practical way out for companies like Yahoo is to be

able to say to China that U.S. law forbids them from complying with requests to turn over the names of dissidents.

Congress should also act to discourage Internet companies from censoring content at the request of repressive governments. At the very least, such companies should be denied taxpayer financing for their foreign operations from OPIC and EximBank. You might consider whether they should be banned from federal procurement.

Finally, the Congress and the administration should encourage Internet and information technology companies to develop an industry wide code of conduct governing their behavior in repressive societies. Such a code would strengthen the companies' leverage in dealing with the Chinese and other similar governments, since it would allow them to present a united front. Similar initiatives have been pursued in other industries—a few years ago, for example, several of the world's leading oil and mining companies developed with nongovernmental organizations and the U.S. and British governments a set of principles to make their operations consistent with international human rights standards. If such old economy companies as Exxon and BP can agree on their responsibilities in difficult environments like Nigeria and Angola, surely the champions of free speech in the new economy can do the same in China, in the Middle East and everywhere free expression is threatened.

That we even have to suggest such a thing to companies that came into being with a professed commitment to bucking the status quo and to standing up for freedom is sad, Mr. Chairman.

I say that as a representative of an organization that was founded in the 1970s to stand up for human rights behind the Iron Curtain, with funding and support that came in part from people like Robert Bernstein, who made their money in the book publishing industry. Now, American publishing houses are not charities; they exist to make money, like any other company. But they are also in a business that depends on the free exchange of ideas. Their first thought in those days was not "How can we ingratiate ourselves with the Soviet Union so that we can sell books there?" It was, "how can we support free expression so that in the long run everyone has free access to the product we sell?" That was the right thing to do. And it was the sensible thing to do.

I have hoped that the Internet companies would recognize that as well. But as they have not, the time has come for the Congress to say that some principles are not optional.

Written Statement of:

John G. Palfrey, Jr.
Clinical Professor of Law & Executive Director
Berkman Center for Internet & Society, Harvard Law School

Congressional Human Rights Caucus Members' Briefing
on the subject of human rights and the Internet in China
February 1, 2006

Mister Chairman, Distinguished Members of the Caucus:

My name is John Palfrey. Thank you for the leadership of this Caucus in drawing attention to the relationship between the Internet and human rights in China and for the opportunity to speak with you today. I am here today as a member of a team of researchers, called the OpenNet Initiative, that has been conducting empirical testing of China's Internet filtering regime for the past several years and monitoring the involvement of United States companies in that regime. My colleagues Ronald Deibert of the University of Toronto, Rafal Rohozinski of the Advanced Network Research Group of the Cambridge Security Program, University of Cambridge, and Jonathan Zittrain of the University of Oxford and Harvard Law School, are also principal authors of the OpenNet Initiative's work. We have also studied in depth the filtering regimes of states in the Middle East, the former Soviet republics, and parts of East Asia. I am joined today by my colleague Nart Villeneuve, the Director of Technical Research at the Citizen Lab at the University of Toronto.

Today the Caucus considers human rights with respect to the Internet in China. I applaud your efforts to shine a spotlight on this important matter. I hope that your efforts, and those of your colleagues, will lead to new ways to work together to achieve our common goal of global economic development that is consistent with the values that we hold dear as Americans and as citizens of our increasingly connected world.

While China seeks to grow its economy through use of new technologies, the Chinese state's actions suggest a deep fear of the sometimes disruptive effects of free and open communications made possible by the Internet – particularly on topics of human rights. This fear has led the Chinese government to create the world's most sophisticated Internet filtering regime. One of the topics commonly blocked is information related to human rights, including the website of the respected NGO, Human Rights Watch.

Increasingly, the Chinese state has turned to private companies that control parts of the middle of the network to assist in its filtering and surveillance practices. These companies find themselves today in an awkward, if not untenable, position on this issue of ethics and human rights. Individual companies can be isolated and pressured by the

filtering state and undercut by competitors willing to comply with surveillance and filtering requests.

United States technology companies, which have led the Internet revolution from the start and have brought us many of its extraordinary benefits, are now in the uncomfortable posture of helping to carry out Internet filtering practices. These companies also find themselves under pressure to turn over sensitive personal information to law enforcement officials, in circumstances where these companies would not turn over the information here in the United States.

Private technology companies cannot today participate in these marketplaces without consequences based upon their actions. Human rights are implicated. Companies in this position have an obligation to figure out what it means to act ethically when they are doing business in a place like China. They also have a self-interest in having a common code of practice to which they can point and rely upon in resisting abusive filtering and surveillance requests. The United States Congress is right to pay attention.

Despite what may seem to be a common set of problems, United States technology companies should not be lumped into a single category when it comes to their participation in Internet filtering and surveillance practices. Plainly, there are different issues at stake when a company is making technology products that are designed to carry out filtering regimes in other countries around the world as compared to a company that is making general-purpose technology that happens to be used to filter or spy on Internet-based communications. Surely there are differences between the company that offers a limited online service in China and collects no personally identifiable data as compared to a company that not only collects large amounts of such data but turns it over prior to a formal legal action. Surely we would distinguish between a company that folds at the first hint of controversy and the company that draws lines in the sand and puts its license to do business in that state in harm's way. There are ethical lines to be drawn between various kinds of technology companies that are doing business in China. These lines will help to shape what we believe to be good public policy on this matter.

In terms of how to move forward, there are several options.

First, and most appealing as a next step, is for the United States information technology industry, perhaps with other players from states that face this problem, to work together to try to sort out a common ethical pathway. I, and some of my colleagues at the Berkman Center at Harvard Law School, believe that we should explore the development of a set of principles that would guide businesses that are offering services in states that filter extensively and spy on Internet conversations and give them a base of support for resisting abusive surveillance and filtering requests.

There are a number of things that United States technology companies can do to make their actions more transparent to users, more protective of civil liberties, and more accountable to all of us. Yesterday, Microsoft announced a policy with respect to content hosted on their popular MSN Spaces blog software in China, which is very much a step in the right direction.

The Chinese state's filtering systems lack transparency in nearly every sense. In addition to limiting what Chinese citizens can come to know about the censorship process, this lack of transparency complicates the task of monitoring its filtering regime.

Most important, this lack of transparency contributes mightily to the climate of self-censorship. Chinese officials very rarely admit that the state censors Internet content. Officials do not disclose at any level of granularity what material it targets through the filtering regime. United States technology companies can help on this transparency front by how they carry out their blocking.

Second, it may be the case that the Congress could develop a corollary to the Foreign Corrupt Practices Act that would guide – and tie the hands of – United States technology companies doing business under these circumstances. Such a step is risky on many levels and should be taken only with great care, and only if our technology industry is unable to work out the problem on its own.

Third, the United States ought to consider making this human rights issue a matter of foreign trade policy or other forms of international negotiation. In the Internet context, the United States ought to stop worrying about the future of the Internet Corporation for Assigned Names and Numbers and should make Internet filtering and surveillance the key Internet governance issue on the world stage.

The best outcome is not to ban the involvement of United States technology companies in China outright. The best outcome would be for our technology companies to be able to compete in these marketplaces – with their best-in-the-world offerings – without having to compromise our values and without having to become complicit in Internet censorship and surveillance.

In conclusion, we ought to see this issue not as a crisis, but rather as an opportunity. Internet technologies, developed by the likes of Microsoft, Yahoo!, Google, Cisco, and many others, are doing terrific things for democracy around the world. At the same time, the People's Republic of China's Internet filtering and surveillance regime has the greatest effect on the freedom of expression, and on the efforts of human rights workers, of any filtering regime throughout the world.

We need to come together to figure out how to ensure that these companies and their technologies are indeed a force for greater democratic participation, not pushing against it. These companies should be, and can be, the darlings of the human rights community for what they can do for human rights in places like China. It doesn't happen to be the case today, but I have no doubt that we can get to that point through collaboration that is grounded in honesty, openness, and transparency.

-- End of Written Testimony --

Appendix:

The OpenNet Initiative's Methodology for Studying Internet Filtering in China.

Members of our consortium have been collecting data on China's Internet filtering regime since 2002. The data included in this report have been updated as recently as this week. As the Chinese government has developed more sophisticated means of filtering, we too have developed more sophisticated and comprehensive means of testing their filtering efforts. Since our last study, our testing methods have become substantially more fine-grained and reliable.

To gauge how Internet filtering likely affects the average Chinese Internet user, ONI employs a variety of means to test blocking and censorship and to ensure data integrity. We test filtering from different points on China's network, in different geographic regions, across time. The resulting data allow us to conduct rigorous longitudinal analysis of Internet blocking in China. We examine both the response that users receive from the network and from the Web servers involved and information about the route that a request takes on its way from a user to a Web server – allowing us to pinpoint exactly where information is censored and controlled. While it is impossible to paint a flawless picture of China's Internet filtering efforts at any given time, we are increasingly confident that our data present an accurate snapshot of China's Internet filtering regime today.

We have tested China's Internet filtering regime using four methods. Under Nart Villeneuve's leadership, ONI developed and deployed an application to test within China what content is, and is not, blocked by the state's system. Volunteers installed and ran this application on their home computers to allow ONI to probe China's filtering from a wide range of access points inside the country. Our volunteers also ran manual checks for access to web sites.

Second, we accessed proxy servers in China to duplicate and augment this in-state testing of whether or not a citizen could access a certain web site. Proxy servers are points in China's network that act to aggregate and respond to user requests for content. Accessing a proxy server in China allows ONI to browse the Internet as though we were in China, even though we are physically located in another country. Through proxies, we are able to obtain a random sampling of Web content – and censorship – across multiple networks and service providers.

We have also explored whether China blocks other types of Internet-related communications. Anecdotal evidence has suggested for a long time that China blocks certain e-mail communications and that Web logs – or "blogs", which are personal online journals, often kept by increasingly famous activists – have been more recently targeted by the Chinese government for blocking.

To test these hypotheses, we published content on blogs on three of China's most popular blog providers to evaluate the services' keyword filtering mechanisms. We then later sought to access this blog content that we had published.

Finally, we sent a series of test e-mail messages to, and from, accounts hosted by several Chinese ISPs. These messages contained content on sensitive topics – such as political dissidents, objections to the state's repression of the Tiananmen Square

protests, and religious persecution – typical of e-mails sent by human rights organizations.

In addition to employing these technical methodologies, we have closely studied the legal and policy regimes in place in China. The insights of many scholars and activists, both inside China and elsewhere, guided our research and provided quality assurance.

Topics Censored by the Chinese Filtering Regime.

China filters Internet content on a broad array of topics. The censors particularly target sensitive political topics for blocking. To determine precisely what is blocked, we created a keyword list of terms on sensitive topics, such as the Falun Gong spiritual movement, the Taiwanese independence movement, and criticism of China's government and leaders. We used the Google search engine to compile a list of large numbers of sites related to these keywords. Our volunteers then attempted to access these sites from within China using our testing application.

Some of the most noteworthy of the topics censored include:

- Information online related to opposition political parties (more than 60% of Chinese-language sites tested were blocked);
- Political content (90% of Chinese-language sites tested on *The Nine Commentaries*, a critique of the Chinese Communist Party, and 82% of sites tested with a derogatory version of Jiang Zemin's name were blocked);
- The Falun Gong spiritual movement (44 – 73% of sites tested, in both English and Chinese languages);
- The Tiananmen Square protest of June 4, 1989 (at least 48% of Chinese-language sites tested, and 90% of sites related to the search term "Tiananmen massacre");
- Independence movements in Tibet (31% of tested Chinese-language sites), Taiwan (25% of tested Chinese-language sites), and Xinjiang province (54% of tested Chinese-language sites); and,
- Virtually all content on the BBC's web properties and much of the content published online by CNN.

China has issued official statements about its efforts to limit access to Internet pornography. However, we found that less than 10% of sites related to searches for the keywords "sex," "pornography," and "nude" were blocked. This imprecision, when compared either to the effectiveness of China's censoring of political content or to the relatively thorough blocking of pornographic materials by states in the Middle East, suggest that blocking pornography is nowhere near the imperative that controlling political speech is in China. It also suggests that China's war on pornography may be focused more on closing domestic sources of pornography than on filtering foreign sites that are providing pornographic content.

Our testing also found evidence that China tolerates considerable overblocking – filtering of content unrelated to sensitive topics, but located at URLs or with keywords similar to these subjects – as an acceptable cost of achieving its goal of controlling Internet access and publication. China has managed over time to reduce the rate of overblocking as its filtering technologies have improved.

Types of Communications Affected by China's Filtering Regime.

China's commitment to content control is revealed by the state's efforts to implement filtering for new methods of communication as they become popular. Most states that filter the Internet do an ineffective job of blocking access to certain web sites, and stop there.

While China's blocking of World Wide Web sites is well-known, much less is known about the extent to which China blocks other forms of Internet-based communications. As Web logs ("blogs") became popular in 2004, the state initially closed major Chinese blog service providers until they could implement a filtering system. When these providers re-opened, their service included code to detect and either block or edit posts with sensitive keywords. Similarly, on-line discussion forums in China include both automated filters and human Webmaster inspections to find and remove prohibited content. Most recently, China moved to limit participation in university bulletin board systems (BBS) that had featured relatively free discussion and debate on sensitive topics. The Chinese filtering regime also causes the blockage, or dropping, of e-mails that include sensitive terms. Our testing of e-mail censorship suggests that China's efforts in this area are less comprehensive than for other communications methods, though reports from the field suggest that the fear of surveillance and blockage of e-mails is a serious issue for many activists regardless of the precise extent of the censorship itself.

One of the most intriguing questions, as yet unanswered, is whether emerging new technologies will make Internet filtering harder or easier over time. A new, emerging crop of more dynamic technologies – centered on the fast-growing XML variant RSS, which is a means of syndication and aggregation of online content, such as weblog entries and news stories from major media outlets – should make filtering yet harder for the Chinese and for other countries that seek to control the global flow of information. The cat-and-mouse game will continue.

The Legal Context of Filtering in China.

China's intricate technical filtering regime is buttressed by an equally complex series of laws and regulations that control the access to and publication of material online. While no single statute specifically describes the manner in which the state will carry out its filtering regime, a broad range of laws – including media regulation, protections of "state secrets," controls on Internet service providers and Internet content providers, laws specific to cybercafés, and so forth – provide a patchwork series of rationales and, in sum, massive legal support for filtering by the state. The rights afforded to citizens as protection against filtering and surveillance, such as a limited privacy right in the Chinese Constitution, which in other situations might provide a counter-balance against state action on filtering and surveillance, are not clearly stated and are likely considered by the

state to be inapplicable in this context. For the most part, the Chinese legal regime is not transparent, in the sense that it does not describe the filtering regime.

Our analysis of China's legal regime indicates a significant expansion in the number of statutes, regulations, and regulatory bodies involved in oversight and control of Internet access and content since 2000. These rules often appear to be arbitrary and are certainly extraordinarily burdensome, such as rules that call for multiple licensing and registration requirements imposed upon Internet content providers.

China's legal system imposes liability for prohibited content on multiple parties: the author who creates it, the service provider who hosts it, and the end user who accesses it. This combination of transaction costs and broad liability has a substantial chilling effect on on-line communication.

We are cognizant that, while we have taken great care in our legal analysis of China's filtering regime as it appears on the books, our report may not describe the law as it applies on the ground. Political stability is clearly more important than legal justification for the state's actions, as a comparison of China's filtering regime to the corresponding legal framework demonstrates.

A Comparison of China with Other States that Filter.

Our studies have compared the Internet filtering practices of a series of national governments in a systematic, methodologically rigorous fashion. A primary goal of this research is to reach useful, substantive conclusions about the nature and extent of Internet filtering in states that censor the Internet and to compare practices across regions of the world. Over the course of the next several months, we will release a series of extensive reports that document and provide context for Internet filtering, previously reported anecdotally, in each of the dozen or so countries that we have studied closely. The new reports released to date – which document filtering in Saudi Arabia, the United Arab Emirates, and Bahrain as well as in China – will be followed shortly by other studies of other states in the Middle East, East Asia, and Central Asia.

Filtering regimes – and their scope and level of effectiveness, respectively – vary widely among the countries we have studied. Filtering is practiced at some level by most countries; it is best thought of as a continuum of behavior rather than a binary, on-off approach to content control. Some countries employ only symbolic filtering, and depend on legal or social pressures to constrain content. These states include Bahrain and Singapore, which block only a few sites that are primarily pornographic in nature. Other countries demonstrate limited blocking but, because of an unsophisticated approach to filtering, also censor large numbers of unrelated sites. This inadvertent filtering, known as "overblocking," was demonstrated by South Korea when it sought to prevent access to sites promoting North Korea. Finally, many countries employ a mix of commercial software (from American companies such as Secure Computing and Websense) to control content such as pornography and gambling while also customizing their block lists to target prohibited political, religious, and social content.

China, as documented in a number of studies and supported by the our findings, institutes by far the most intricate filtering regime in the world, with blocking occurring at multiple levels of the network and covering content that spans a wide range of topic areas. Though its filtering program is widely discussed, Singapore, by contrast, blocks

access to only a small handful of sites, mostly pornographic in nature. Most other states that we are studying implement filtering regimes that fall between the poles of China and Singapore, each with significant variation from one to the next. These filtering regimes can be properly understood only in the political, legal, religious and social context in which they arise.

A complete study of Internet filtering in China, as of 2005, may be found at http://www.opennetinitiative.net/china/.

The OpenNet Initiative is a collaborative partnership between three leading academic institutions: the Citizen Lab at the Munk Centre for International Studies, University of Toronto; Berkman Center for Internet & Society at Harvard Law School; and the Advanced Network Research Group at the Cambridge Security Programme, University of Cambridge.

STATEMENT SUBMITTED FOR THE RECORD BY MR. T. KUMAR, ADVOCACY DIRECTOR FOR ASIA AND THE PACIFIC, AMNESTY INTERNATIONAL USA

Thank you Mr. Chairman and members of the Congress; Amnesty International (AI) is pleased to submit this testimony for the record at this important and timely hearing. Despite AI's reporting on the issue of Internet censorship and related human rights abuses since 1999, the Chinese Government's determination to crack down on peaceful Internet users seems only to have grown. This trend is disturbing but not surprising, given the Chinese Government's widely acknowledged practice of silencing political dissidents and others who express their views peacefully.

What is new about recently reported abuses is the willingness of U.S.-based companies to join hands with the Chinese Government in aiding such practices.

WHAT DOES CENSORSHIP LOOK LIKE IN CHINA?

There is a tendency in public discourse to sanitize the issue of freedom of expression and access to information in China, creating the perception that it is simply about not having access to a few controversial websites. This is far from the reality. In China, individuals can be sentenced to death for publishing information on the Internet that the government considers a "state secret"—the definition of "state secret" can change on a daily basis, and can include important public health information (for instance on SARS or HIV/AIDS) or simply an opinion about a labor dispute. Scores of people have been imprisoned in China for using the Internet, and, of those arrested, some have died as a result of torture by the police. Those detained to date range from political activists and writers to Falun Gong practitioners and members of other religious groups banned by the authorities.

Individuals who are active on the Internet, and who challenge the government, can experience continuous harassment. Such harassment includes but is not limited to temporary detention, threats to one's family, business or career, and being followed and intimidated by the police.

INTERNET COMPANIES' ASSISTANCE TO THE CHINESE GOVERNMENT

Several international companies provide Internet services in China and many have headquarters within the United States. Some of these companies, including Cisco Systems and Sun Microsystems, have helped to build the infrastructure that makes Internet censorship possible while others, including Yahoo!, Microsoft, and Google are increasingly complying with government demands to actively censor Chinese users by limiting the information they can access.

In the most egregious case that we know of, Yahoo! sacrificed the privacy of one of its users to facilitate his subsequent imprisonment for peacefully expressing opinions over the Internet. These companies not only put profits above principle but also willingly ignore international human rights standards. Amnesty International is concerned that, in the pursuit of new and lucrative markets, these IT companies are contributing to human rights violations. Unless a strong action is taken by the U.S. Government and the Congress, this type of practice will not only increase but is likely to move into other areas, which will lead to disastrous impacts on the well-being of the Chinese people and significant risks for U.S. companies operating overseas.

YAHOO DENIES U.S. FAMILY ACCESS TO DECEASED MARINE'S EMAILS

While American IT companies seem to be falling over each other to help the Chinese Government in censoring its citizens, here in the United States, Yahoo! denied a family access to their deceased son's email, citing privacy concerns. Their son was Justin Ellsworth, a 20-year old Marine killed in November by a roadside bomb while assisting civilian evacuations before a large-scale military offensive against insurgents in the city, said a report in the Detroit Free Press. But when Ellsworth's father John tried to recover his son's email account, he was barred due to Yahoo!'s seemingly unflinching policy of not giving personal user information to anyone besides the account holder. Apparently, this policy is only circumvented when the request comes from one of the world's most repressive governments, with the goal of stifling free speech.

DOUBLE STANDARDS AT HOME AND ABROAD

There is a tendency in the international business community to deal with the Chinese Government on the basis of a different set of standards. The above mentioned John Ellsworth's case is only one example. Human rights obligations apply to all states equally. Furthermore, nuanced interpretations of international standards on censorship are well documented, including by Amnesty International. This problem

extends well beyond the IT sector. Nonetheless, this sector raises particularly troubling concerns, considering how lightly Internet technologies are regulated. When faced with the prospect of challenging the Chinese Government on their repressive practices, companies often claim that the Government is simply too powerful and that they have no alternatives but to comply with their requests, even those that run counter to international human rights norms, the company's mission or standards, U.S. law, or even China's own constitution. If U.S.-based IT companies are to do business in China (or anywhere else), they ought to apply their business standards universally. Another argument we often hear is that the Chinese Government will eventually ease its censorship, and that U.S. companies need to be poised for this imminent change. But there is absolutely no evidence that this is likely to happen. In fact, there is significantly more evidence to the contrary. Though our IT companies like to pretend that there is no stopping the swift march of information in China, we should not underestimate the state machinery of repression so deeply embedded in China's infrastructure. The Chinese Government's investments in Internet controls appear to be keeping pace with technological developments, and for companies to claim that such control is not sustainable for the Chinese is both naïve and dangerous. If we permit American companies to give in to the Chinese on censorship, their infrastructure for control only becomes more powerful. To ensure that this does not happen, we recommend the development of U.S. legislation regulating U.S. companies overseas, and other companies publicly traded on U.S. stock exchanges (which would include Baidu, the primary Chinese competitor), prohibiting them from complying with violations of freedom of expression and freedom of information by repressive regimes.

Until the time that such regulations are instituted, in situations where companies claim exemption from international standards in order to do business in an emerging economy, those companies should be required to justify their presence in the country and disclose their double standards, while working in a multi-stakeholder process to develop and advance improved standards. As reported widely in the U.S. press on January 31, 2006, Microsoft has publicly stated their hope for the arrival of "a broad set of principles for (the) full range of Internet technology." We support this recommendation and would expect the process to be open and transparent, including participation by NGOs as well as companies and government, and that it would provide not only principles, but explicit guidelines for implementation and evaluation.

THE MYTH OF "NET POSITIVE" IMPACT

IT companies often point to the "net contribution" that their company's presence has had on the proliferation of freedom of expression and information in China. While the Internet has undoubtedly increased access to these freedoms generally, there is no evidence we have seen to demonstrate that the presence of U.S.-based IT companies has accomplished any more for the Chinese people than state companies such as Baidu, the leading provider of internet technology in China. If every company operating in China is complying with the same standards of repression, it is hard to understand how using a different company's search page to find the exact same limited information provides any added benefits to Chinese users. What is clear is that it provides added benefits to the U.S. company, in terms of profits.

Despite their claims, it appears that these U.S. companies are not very concerned about promoting the welfare of Chinese citizens. Take the recent announcements, first by Google and then by Microsoft, that they would provide some disclosure to their users about the fact that their content had been censored "according to local laws and regulations." As reported in The New York Times on February 1, this new policy would not have prevented the censoring of the Chinese blogger, Zhao Jing. So what is the net benefit of this policy to the Chinese people? They still cannot access information, and they do not learn anything specific about the nature of the censorship, such as which sources were blocked, for what specific aspect of the law. One thing the companies claim is true: each time the disclosure pops up the Chinese users receive a reminder that their government is the primary agent of that censorship (a reminder they probably don't need). But the message they receive even more clearly is that now America's most prominent IT companies are partners in that repression, and that they find it acceptable. This is a huge blow for human rights, and for the perception of American values abroad.

We are dismayed that these companies would claim the ethical high ground for a decision that appears to be purely financial. In order for the Internet to fulfill its role as a tool of democratization, a "liberating technology" as Bill Gates referred to it at Davos, companies must UNIVERSALLY ensure freedom of expression is protected and access to information is not suppressed. Where companies cannot, the

burden of evidence should be on them to demonstrate the net positive impact of their presence, if such an impact truly exists.

EXAMPLES OF U.S. IT COMPANIES AIDING HUMAN RIGHTS ABUSES

In November 2002, in the report *State control of the Internet in China*, AI cited several U.S. companies—including Cisco Systems, Microsoft, and Sun Microsystems—which had reportedly provided technology used to censor and control the use of the Internet in China. In January 2004 Amnesty released an updated report, *Controls tighten as Internet activism grows*, which indicated that there was a dramatic rise in the number of people detained or sentenced for Internet-related offences, an increase of 60 per cent in 2003 as compared to the previous year's figures. In addition, an unknown number of people remained in detention for disseminating information about the spread of Severe Acute Respiratory Syndrome (SARS) over the Internet. Additionally:

YAHOO!

Also of grave concern are the allegations that Yahoo! has cooperated with Chinese authorities in events which led to the detention of Shi Tao, a Chinese journalist. This case is particularly disturbing because the company provided specific information about an individual user. Linking email to a specific user is information only Yahoo! would have access to, and, seeing as such information was not demanded by a court order, it appears that its release was the result of nothing more than a political demand. Mr. Shi was imprisoned solely for the legitimate exercise of his right to seek, receive and impart information, as guaranteed under Article 19 of the International Covenant on Civil and Political Rights, which China has signed but not ratified. According to the court transcript of the *Changsha Intermediate People's Court of Hunan Province Criminal Verdict*, evidence presented by the prosecutor that led to the sentencing of Mr. Shi included account-holder information provided by Yahoo! Holdings (Hong Kong) Ltd. Yahoo! has admitted that their subsidiary provided this evidence by correcting the record to state that the information was provided not directly by Yahoo! Holdings (Hong Kong) Ltd. but by Yahoo! China, which is held by Yahoo! Holdings (Hong Kong) Ltd. On April 27, 2005, Mr. Shi received a ten-year prison term for sending information about a Communist Party decision through his Yahoo! email account to a website based in the United States. Mr. Shi's appeal was denied on June 2, 2005.

MICROSOFT

According to recent reports, Microsoft's search engine MSN blocks searches under certain key words, including "democracy", "freedom", "human rights", Falun Gong", "June 4", and "demonstration", among others. In China, users of the product Microsoft Spaces are also prohibited from using these and other words on weblogs they create. As a result, websites and webpages dealing with human rights, including those of Amnesty International and other human rights organizations, are inaccessible to internet users in China. In January 2006, stories surfaced that Microsoft had cooperated with Chinese authorities in shutting down a controversial blog.

GOOGLE

Most recently, Google launched a self-censoring Chinese search engine—the latest in a string of examples concerning global Internet companies caving-in to pressure from the Chinese government. The service curtails the rights of Chinese Internet users to the freedom of expression and freedom of information enjoyed in other countries. Amnesty International's Secretary General, Irene Khan, released a statement from the World Economic Forum in Davos, Switzerland, saying:

> "While acknowledging that Google has taken a number of steps to ensure access of Chinese users to the Internet, Amnesty International is nonetheless dismayed at the growing global trend in the IT industry.
>
> "Whether succumbing to demands from Chinese officials or anticipating government concerns, companies that impose restrictions that infringe on human rights are being extremely short-sighted. The agreements the industry enters into with the Chinese government, whether tacit or written, go against the IT industry's claim that it promotes the right to freedom of information of all people, at all times, everywhere."

OUR COMMUNICATIONS WITH THE INTERNET COMPANIES:

We have communicated with several IT companies about our concerns, including those named above. So far we have not received any substantive responses from these companies that address our concerns. In many cases these are the same companies that have refused the invitation to attend today's testimony. We are shocked by their willingness on the one hand to collude with the repressive practices of the Chinese Government, and unwillingness to stand accountable in front of the democratic government of their home country.

OVERVIEW

Since the commercialization of the Internet in China in 1995, China has become one of the fastest-growing Internet markets in the world. The number of domestic Internet users has been doubling every six months.

With the introduction of the Internet, news reaches China from a multiplicity of sources enabling people to form opinions, analyze and share information, and communicate in ways previously unknown in China. Lively on-line debate characterized the start of the Internet in China. However, the potential of spreading new ideas through the Internet has led authorities to take measures to control its use.

The authorities have introduced scores of regulations, closed Internet cafes, blocked e-mails, search engines, foreign news and politically-sensitive websites, and have recently introduced a filtering system for web searches on a list of prohibited key words and terms.

Those violating the laws and regulations which aim to restrict free expression of opinion and circulation of information through the Internet may face imprisonment and according to recent regulations some could even be sentenced to death. As of January 7, 2004, Amnesty International had recorded the names of 54 people who had been detained or imprisoned for disseminating their beliefs or information through the Internet—a 60 percent increase as compared to figures recorded at the end of 2002. Current information suggests that roughly fifty plus internet-related prisoners continue to be held in China. In addition, an unknown number of people remain in detention for disseminating information about the spread of Severe Acute Respiratory Syndrome (SARS) over the Internet. Prison sentences ranged from two to 12 years.

Internet access expanded considerably in China during 2003. According to official statistics, the number of Internet users had risen to 79.5 million by December 2003 from 59.1 million users in December 2002—an increase of 34.5 percent. According to the China Internet Network Information Center, the number of Internet users reached 111 million by 2005. This has presented the authorities with greater challenges in their attempts to censor and control the online activities of Internet users. During 2003, there was a growing trend towards assigning greater responsibilities of surveillance and monitoring to a variety of companies in China such as Internet Cafes, Information Service Providers (ISPs) and other enterprises.

Though it appears that Internet activism is continuing to grow in China as fast as the controls are tightened, this should not be misconstrued as evidence that company compliance with state sanctioned repression somehow does more good than harm. Recently, there have been signs of Internet users acting increasingly in solidarity with one another, in particular by expressing support for one another online. Such expressions of solidarity have proved dangerous, as a growing number of people have been detained on the basis of such postings.

THE INTERNET IN CHINA—FACTS AND FIGURES

- China joined the global internet in 1994. It became commercially available in 1995.
- By 2005, the number of internet users reached 111 million.
- China is second only to the United States in the number of Internet users.
- China's Internet market is likely to become the largest in the world within four years.
- More than 40% of internet users are based in prosperous cities, particularly Beijing, Shanghai, Shenzhen and Guangzhou.
- Internet users are predominantly young, with almost 40% aged 24 or under.
- The proportion of female users continues to increase and now represents over 39 per cent of all users.
- Initially, Internet users were predominantly those with a high school or college education. But those without a college education now make up 68.3% of the total, indicating a broader spectrum of use within China.

- Officials at the Asia-Pacific Economic Conference (APEC) in February 2001 predicted that 70 percent of Chinese foreign trade companies will be able to conduct import and export business via electronic means by the year 2005.
- Since 1995 more than 60 rules and regulations have been introduced covering the use of the Internet.
- In January 2001, a new regulation made it a capital crime to "provide state secrets" to organizations and individuals over the Internet.
- 30,000 state security personnel are reportedly monitoring websites, chat rooms and private e-mail messages.
- Following a fire in a Beijing cybercafe in 2002, the state shut down 150,000 unlicensed cybercafes. Between October and December 2004, China closed over 12,000 Internet cafes.
- On 26 March 2002, the authorities introduced a voluntary pledge, entitled, *A Public Pledge on Self-Discipline for the China Internet Industry*, to reinforce existing regulations controlling the use of the Internet in China. Over 300 Chinese Internet business users have reportedly signed the public pledge, including the U.S.-based search engine Yahoo!
- In July 2002, a *Declaration of Internet Users' Rights* was signed and published by 18 dissidents calling for complete freedom of the Chinese people to surf the Internet.

IMPRISONMENT FOR USING THE INTERNET

At least 54 Chinese Internet users are imprisoned after often unfair trials solely for peacefully exercising their right to freedom of expression and opinion, in violation of international standards. They include people who have expressed their views or circulated information via the Internet or email. Those detained for downloading information from the Internet, expressing their opinions or circulating information on the Internet or by email include students, political dissidents, Falun Gong practitioners, Tibetan exiles, workers, writers, lawyers, teachers, civil servants, former police officers, engineers, and businessmen.

Signing online petitions, calling for reform and an end to corruption, planning to set up a pro-democracy party, publishing 'rumors about SARS', communicating with groups abroad, opposing the persecution of the Falun Gong and calling for a review of the 1989 crackdown on the democracy protests are all examples of activities considered by the authorities to be "subversive" or to "endanger state security". Such charges almost always result in prison sentences.

Individuals who are active on the internet, and who challenge the government, can expererience continuous harassment. Such harassment includes but is not limited to temporary detention, threats to one's family, business or career, and being followed and intimidated by the police. Many of those included in this report have been held for long periods, sometimes for over a year, awaiting a formal trial and for some there has been a long delay between trial and sentencing. All are believed to have been denied full and adequate access to lawyers and their families, particularly during the initial stages of police detention, and several have reported being tortured or ill-treated. In addition, four prisoners directly linked with Falong Gong and charged with Internet related crimes have died in custody. Such violations of the right to a fair trial and to freedom from torture or ill-treatment often contravene provisions of China's Criminal Procedure Law as well as international human rights standards.

The following cases illustrate such failings. They also show how the arrest of one Internet activist can result in spiralling arrests of others who dare to express their support or solidarity online. Several of these cases have been documented by Amnesty International. These cases show the systematic nature of state persecution of Internet activists.

Huang Qi, is notable for being the first person in China to be arrested for posting articles concerning human rights and political issues on his own website. After his trial in August 2001, he continued to be detained for almost two years before his sentence was finally announced on 9 May 2003—five years' imprisonment for "inciting subversion". By that time Huang Qi had spent a total of almost three years in detention.

It remains unclear why it took so long for the sentence to be announced after the trial. Huang Qi filed an appeal on May 18, 2003, pointing out that China's Constitution guarantees the right to freedom of speech and of the press. During his appeal hearing, prison guards reportedly held him down by the throat as he tried to speak in his defense. In August 2003 his appeal was turned down and the five-year sentence upheld.

Amnesty International was concerned to note that according to the court verdict, the prosecution cited evidence which included reference to the posting of an Amnesty International document on Huang Qi's website. Amnesty International believes that merely publishing names of individuals imprisoned following the 1989 pro-democracy protests on the Internet can never amount to "inciting subversion".

After his appeal Huang Qi was transferred to Chuanzhong high security prison, in Nanchong in Sichuan Province. Following a visit by representatives of the international non-governmental organization Reporters Without Borders in October 2003, Huang Qi was reportedly placed in solitary confinement and then moved to a punishment cell. He is reported to be in poor health. On June 4, 2005, Huanq Qi was released from prison, but remains confined to his parents' home, three hours from his wife and family's home in Chengdu.

- In December 1999 Wang Youcai, founder of the China Democracy Party (CDP), was sentenced to 11 years imprisonment for subversion. Two of the accusations against Wang Youcai involved sending e-mail to Chinese dissidents abroad and accepting overseas funds to buy a computer.
- Lin Hai, a computer engineer from Shanghai, was arrested in March 1998 and is considered to be the first person to have been sentenced for the use of the Internet in China. He was accused of providing 30,000 email addresses to VIP Reference, a U.S.-based on line pro-democracy magazine, and charged with subversion and sentenced to two years in prison in June 1999.
- Members of the Falun Gong spiritual movement, banned in July 1999 as a 'heretical organization', have used the Internet and e-mail to circulate information about repression against the group. Some have been arrested as a result. The Chinese authorities have now shut down the group's websites and blocked overseas websites. At least 14 Falun Gong practitioners have been detained and imprisoned for Internet-related offences.

Amnesty International is concerned about the growing number of individuals being detained, charged and imprisoned for doing nothing more than peacefully expressing their views and opinions on the Internet, including those who have expressed support or solidarity with Liu Di or with detained Internet activists in general. AI continues to call for their immediate and unconditional release.

Amnesty International has investigated the cases of 54 people believed to be prisoners of conscience. They have been detained or are serving long sentences in prison or labor camps for Internet-related offences. Four have died in custody, two of whom reportedly died as a result of torture, and there are reports that others have been tortured or ill-treated in detention.

All were peacefully exercising their right to freedom of expression and opinion. The accusations against them include circulating and downloading articles calling for political and social reform, greater democracy and accountability or redress for abuses of human rights. Most have been charged with "subversion" or membership of a "heretical organization". This latter charge has been used widely against Falun Gong practitioners and members of other Qigong or religious groups banned by the authorities.

DETENTION OF INTERNET USERS IN CONNECTION WITH SARS

In May 2003 it was reported by the official Chinese News Agency, *Xinhua*, that over 100 people had been arrested for "spreading rumours" or "false information" through the Internet or mobile phone text messages about SARS. Little further information is available about these cases and it remains unclear exactly how many remain in detention. Amnesty International has received reports suggesting that two of them, **Luo Yongzhong** and **Huang Qunwei** were both sentenced to three years' imprisonment for publishing "rumours" about SARS on the web.

Amnesty International recognizes that restrictions on certain rights such as the rights to freedom of expression and association may be justified in certain circumstances, including a public health emergency. However, international human rights law requires that the rights to freedom of expression and association can only be limited in a necessary and proportionate way to achieve some legitimate aim, such as to stop the spread of disease, and the onus is on the government to demonstrate why certain restrictions are necessary. The Chinese authorities have failed to provide an explanation to justify taking the extreme step of depriving people of their liberty in connection with the exercise of the right to freedom of expression in the context of the outbreak of SARS. In the absence of a credible, official explanation for these arrests, Amnesty International considers those detained for 'spreading rumors about SARS' to be detained in violation of their right to freedom of expression.

Amnesty International also notes that the Chinese authorities initially prevented any reporting or open discussion about the scale and impact of the virus, reportedly by blocking websites mentioning the word 'SARS'. As the numbers of those infected rose and deaths were reported, rumors began to spread quickly as people began to panic and search for answers to their questions. Under such circumstances and without access to credible, official information about the disease, it is not surprising that many people resorted to e-mail, chat rooms, bulletin boards and short message texting (SMS). At the time of the SARS crisis, Internet use was reported to have risen by 40 percent and mobile phone use by 30 percent.

In the face of widespread pressure from both domestic and international sources, the Chinese authorities eventually changed their policy to allow more accurate public reporting on the spread of the disease. The World Health Organization pronounced that the outbreak was under control in June 2003. However, a new suspected case of SARS was confirmed in Guangdong Province in December 2003 and first reported by the *Southern Metropolitan Daily (Nanfang Dushi Bao)*. The authorities have since reportedly questioned the editor and six staff from the paper, apparently over an unconnected issue of alleged corruption. There are concerns that this questioning may in fact be an attempt to intimidate and harass staff involved with breaking the SARS story without official authorization. Amnesty International calls on the authorities to ensure that the media can report freely on SARS, and other issues of legitimate public concern, without fear of intimidation or human rights violations.

RULES AND REGULATIONS THAT FACILITATE CRACKDOWN

The provisions set out in the Chinese Criminal Law and the recent regulations provide the authorities with the means to monitor and control the flow of information on the Internet, keep track of users, enforce responsibilities on operators and police, and punish those that violate provisions affecting the Internet.

Scores of administrative regulations governing telecommunications and the Internet have been introduced since 1994. Many update or reinforce earlier regulations as the perceived threats and challenges to the authorities of the Internet grow or change.

Many of these regulations, particularly those concerning "state secrets", are broad and ill defined. Their implementation has often been harsh, resulting in arbitrary arrest, imprisonment, sometimes torture, confiscation of equipment, and heavy fines. Since January 2001, those who provide "state secrets" over the Internet to overseas organizations and individuals may be sentenced to death.

Regulations affecting the Internet have been issued by different Ministries within the State Council (the executive arm of central government), and as the responsibility for implementation has widened, many basic provisions of earlier regulations have been reinforced at different levels. New organizations have also been set up to control the use of the Internet, including the State Council's Internet Propaganda Administrative Bureau, which guides and monitors the content of Chinese websites, and the Ministry of Public Security Computer, Monitoring and Supervision Bureau.

KEY LAWS AND REGULATIONS INTRODUCED SINCE 1994

Policing the Internet

In 1994, the State Council issued the *"Safety and Protection Regulations for Computer Information Systems."* These regulations gave the Ministry of Public Security (MPS) overall responsibility for "policing" the Internet *"to supervise, inspect and guide the security protection work; investigate and prosecute illegal criminal cases; and perform other supervising duties"*.

Monthly Reports on User Statistics

In 1997, the Ministry of Public Security issued some far-reaching regulations, *"Computer Information Network and Internet Security, Protection and Management Regulations"* which were approved by the State Council in December 1997 and elaborated on in more recent regulations.

Under these regulations, all Internet Service Providers (ISPs) and other enterprises accessing the Internet are responsible to the Public Security Bureau. Internet companies are required to provide monthly reports on the number of users, page views and user profiles. Internet Service Providers are also required to assist the Public Security Bureau in investigating violations of the laws and regulations. Serious violations of the regulations will result in the cancellation of the ISP licence and network registration. As a result, some ISPs have introduced self-censoring policies to deal with the implementation of these 1997 regulations, including volunteers, who patrol chat rooms and bulletin boards to ensure observance of the regulations.

Prohibition of the Release of "State Secrets"

On January 1, 2000, multiple articles on the release of "state secrets" were passed:

Article 3: All individuals, legal persons and other organizations conducting international interconnection ("users"), Internet units or access units shall abide by these Provisions.

Article 8: The administration of the protection of secrecy of online information shall adhere to the principle of "those who go online shall bear responsibility." *Anyone who provides or disseminates information to internationally networked sites must go through secrecy protection examination and approval.* Agencies which implement the administration of secrecy protection examination and approval and relevant units shall establish and perfect online information secrecy protection examination and approval leadership responsibility systems in accordance with national secrecy protection regulations. Units which provide information shall perfect the secrecy protection examination and approval system in accordance with defined working procedures.

Article 9: *Anyone who gathers information with the intention of providing online information services shall acquire the approval of the unit providing the information, unless it has already been openly issued in other news media.* Anyone carrying out augmentation or updating of online information shall conscientiously enforce a system information secrecy protection examination and verification.

Article 10: *Any unit or user who sets up an online bulletin board system, chat room or network newsgroup shall be examined and approved by the relevant secrecy protection work entity, which shall explicitly define its secrecy protection requirements and responsibilities.* No unit or individual may disseminate, discuss or transmit information which is a state secret on an online bulletin board system, chat room or network newsgroup. Those persons who set up online bulletin board systems, chat rooms and network newsgroups which are open to the public or their superior responsible agencies shall conscientiously perform secrecy protection duties and establish sound administration systems to strengthen supervision and monitoring. Upon discovering any information which involves secrets, measures shall be taken in a timely manner and it shall be reported to the local secrecy protection work agency.

Article 11: Users utilizing electronic correspondence to carry online information exchange shall abide by the nation's relevant secrecy protection regulations, and shall not take advantage of electronic correspondence to transmit, transfer or forward on information which is a state secret. Internet units and access units shall explicitly define secrecy protection requirements and perfect administration systems for users of the mail servers which they administer.

Article 12: *Internet units and access units shall make secrecy protection education one of the primary components of international interconnection technical training.* Contracts entered into between Internet units and access units and access units and users and user manuals shall clearly stipulate provisions that national secrecy protection laws shall be obeyed and the divulging of information which is a state secret is prohibited.

i.e. Highlighted above are particularly chilling aspects of the law, clearly intended to intimidate users (both institutional and individual). The vagueness of the definition of state secrets adds to the uncertainty and needed self-censorship of users.

On January 25, 2000, the Bureau for the Protection of State Secrets issued the *"State Secrets Protection Regulations for Computer Information Systems on the Internet".* These regulations prohibit the release, discussion or dissemination of "state secrets" over the Internet. This also applies to individuals and units when making use of electronic bulletin boards and chat rooms. Operators are under an obligation to report "harmful" content to the local Public Security Bureau. All journalists and writers are required to check their written texts with the state-controlled media before publication.

Amnesty International is concerned that laws and regulations on "state secrets" have been used in the past to imprison people exercising peacefully their fundamental rights to freedom of expression and that the prohibition of "state secrets" in the Internet regulations is yet another way of limiting freedom of expression.

Tough new *Measures for Managing Internet Information Services* were issued in September 2000 by the State Council. *"The Measures for Managing Internet Information Services"* regulate the Internet services and promote the "healthy" development of these services. They also stipulate that all Internet Service Providers (ISPs) and Internet Content Providers have to keep records of all subscribers' access to the Internet, account numbers, the addresses or domain names of the websites and telephone numbers used. ISPs are also required to maintain users' records for 60 days and to provide these to "the relevant state authorities" when required.

These measures draw upon the much broader *Telecommunications Regulations of the People's Republic of China* also issued in September 2000 by the State Council.

Article 15 of these Measures describes information that is prohibited:

(1) Information that goes against the basic principles set in the Constitution;

(2) Information that endangers national security, divulges state secrets, subverts the government, or undermines national unification;

(3) Information that is detrimental to the honour and interests of the state;

(4) Information that instigates ethnic hatred or ethnic discrimination, or that undermines national unity;

(5) Information that undermines the state's policy for religions, or that propagates heretical organizations or feudalistic and superstitious beliefs;

(6) Information that disseminates rumours, disturbs social order, or undermines social stability;

(7) Information that disseminates pornography and other salacious materials; that promotes gambling, violence, homicide, and terror; or that instigates the commission of crimes;

(8) Information that insults or slanders other people, or that infringes upon other people's legitimate rights and interests; and

(9) Other information prohibited by the law or administrative regulations.

Amnesty International is concerned that the range of information prohibited by this regulation allows the authorities to restrict freedom of expression over the Internet in a broad and sweeping manner which goes far beyond what would be regarded as legitimate restrictions under international standards.

As part of the ongoing effort to control access to information available on the Internet, new regulations were introduced by the Ministry of Information Industry and the Information Office of the State Council on November 7, 2000. These regulations place restrictions on foreign news and the content of online chat rooms and bulletin boards.

According to these regulations, the State Council's Information Office will supervise websites and commercial web portals such as Sohu.com and Sina.com and media organizations may only publish information which has been subject to controls in line with the official state media.

On December 28, 2000, *The Decisions of the NPC Standing Committee on Safeguarding Internet Safety* were introduced. Under these regulations those spreading rumours, engaging in defamation or publishing "harmful" information, inciting the overthrow of the government or division of the country on the Internet will now be punished according to the law. Prison sentences can be passed against those who promote 'heretical organizations' and leak "state secrets".

Below are additional regulations that show the vagueness of state secrets, which are "harmful to national interest". This allows the government to claim anything as being a state secret.

Legislation	Issuer	Selected Provisions
Interim Provisions on the Administration of Internet Publication (2002)	MII GAPP	**Article 17:** Internet publications may not carry the following types of content: (iii) harming the honor or the interests of the nation; (vi) spreading rumors, disturbing social order, disrupting social stability.
Measures for the Administration of Telecommunication Business Licenses (2001)	MII	**Appendix 2 (III)(iv):** No operators or their employees shall utilize telecommunication networks to produce, copy, promulgate or transmit any information containing the following types of content: 3. Harming the honor or the interests of the nation; 6. Spreading rumors, disturbing social order or disrupting social stability.
Regulations on the Administration of Publishing (2001)	SC	**Article 26:** No publication may contain the following types of contents: (iii) harming the honor or the interests of the nation; (vi) disturbing social order, disrupting social stability.

Legislation	Issuer	Selected Provisions
Notice Regarding Further Strengthening the Administration of Periodicals Relating to Current Affairs and Politics, General Lifestyle, Information Tabloids and Scientific Theory (2000)	GAPP	2. It is strictly prohibited for publications to include any of the following contents: (1) gainsaying the leadership of Marxism, Mao Zedong Thought, Deng Xiaoping Theory; (3) . . . jeopardizing the interests of the nation; (4) . . . influencing social stability; (5) . . . propagating superstition, pseudo-science or incorrect teachings. (6) spreading rumors, producing and distributing false news, interfering in the broader work of the party or the nation; (7) otherwise violating the propaganda discipline of the party or violating the regulations administering the nation's publishing.
Notice Regarding the Further Strengthening the Administration of Selection of Articles for Newspapers and Periodicals (2000)	GAPP	1 . . . . . [Newspapers and periodicals] shall not select articles that contradict the guiding policies of the Party and the nation . . . .
Provisions on the Administration of Internet Electronic Bulletin Services (2000)	MII	**Article 9:** No person may issue any information having the following types of content on an electronic bulletin service: (iii) harming the honor or the interests of the nation; (vi) spreading rumors, disturbing social order or disrupting social stability.
Notice Regarding the Work of Bringing the Periodical Industry Under Control (1997)	GAPP	2(6): In any of the following circumstances where administrative measures have been adopted but there has been no clear improvement, publication should be ceased: (1) Articles have been carried which have severe political errors;
Provisions on the Administration of Electronic Publications (1997)	GAPP	**Article 6:** No electronic publications may contain the following types of content: (iii) jeopardizing the nation's . . . honor or interests.
Measures on the Administration of Safeguarding the Safety of Internationally Networked Computer Information Networks (1997)	MPS	**Article 5:** No unit or individual may utilize the Internet to produce, copy, look up or transmit any of the following categories of information: (v) spreading rumors or disrupting social order; (viii) harming the credibility of a government agency.

Internet Licensing System

Licensing laws were passed on September 25, 2000. *Article 4:* There will be national implementation of a licensing system for commercial Internet information services, and a registration system for non-commercial Internet information services.

No one who fails to be licensed or who fails to comply with registration measures may engage in Internet information services.

Article 14: Providers of internet information services engaged in journalism, publishing and BBS services shall record all information content and the time it was issued, and the internet address or city name; internet access providers shall record information regarding the amount of time each customer was on the internet, the customer's account number, internet address or city name, primary phone number, etc. Providers of internet information services and internet access providers shall

maintain these records for 60 days, and shall make them available to all relevant government agencies examining them pursuant to law.

i.e. even private individuals must register with the government if they want to run a blog, etc. or be shut down or take risk of operating illegally.

Interim Provisions on the Administration of Internet Websites Engaged in News Posting Operations

November 1, 2000. *Article 5:* The legally established websites of central news units, news units of all departments of the central government's agencies and the news units directly under the provinces, autonomous regions and independent municipalities and the municipal people's governments for the provinces and autonomous regions ("news websites") may engage in news posting operations after receiving authorization. *Other news units may not independently establish news websites, but after receiving authorization may establish news web pages and engage in news posting operations on the news website established by a central news unit or a news unit of a province, autonomous region or independent municipality.*

Article 7: Non-news units that establish general interest websites ("general interest non-news unit websites") that possess the qualifications set forth in Article 9 of these Provisions, may engage in operations of posting news promulgated by central government news units, the news units of departments of central government agencies, and the news units directly under the provinces, autonomous regions and independent municipalities, but may not post news from their own sources or news from other sources. Other Internet websites that are established by a non-news unit in accordance with the law may not engage in news posting operations.

Article 8: General interest non-news unit websites that engage in news posting operations shall, in accordance with Article 7 of these Provisions, after receiving examination and approval from the people's government information offices for the provinces, autonomous regions and independent municipalities, submit to examination and verification by the State Council Information Agency.

i.e. no one, or no agency, can transmit any news without formal authorization from the government or a government agency.

The Death Penalty for Offences Related to Use of the Internet

On January 21, 2001, the Supreme People's Court ruled that those who cause "especially serious harm" by providing "state secrets" to overseas organizations and individuals over the Internet may be sentenced to death:

"Those who illegally provide state secrets or intelligence for units, organizations and individuals outside the country through Internet with serious consequences will be punished according to stipulations of the Criminal Law; in especially serious cases, those who steal, make secret inquiries or buy state secrets and intelligence and illegally provide gathered state secrets and intelligence to units outside the country will be sentenced to ten or more years of fixed-term imprisonment or imprisonment for life and their properties may concurrently be confiscated by the state. In cases of a gross violation of law and where especially serious harm is caused to the state and people, law offenders may be sentenced to death and their properties will be confiscated by the state."(17)

To date, no prisoners charged with Internet related offenses have been executed or sentenced to death. The ruling is believed to be a reaction to the revelations contained in The Tiananmen Papers (18) released in the United States. Extracts of these papers were translated and posted on the Internet.

Order to Monitor Use of the Internet

In January 2001, the Ministry of Information Industry (MII) announced new regulations(19) that require Internet Service Providers (ISPs) to monitor more closely peoples' use of the Internet. Software should be installed to ensure that messages are recorded and if they violate the law the ISP must send a copy to the Ministry of Information Industry, the Ministry of Public Security and the Bureau for the Protection of State Secrets.

Tough new regulations introduced by the Ministry of Culture restricting access to the Internet and the operations of Internet cafes entered into force on November 15, 2002. Proprietors of Internet cafes are obliged to install software preventing users from accessing information considered "harmful to state security", as well as disseminating, downloading, copying or browsing material on "heretical organizations" , violence and pornography. Those aged under 18 years old are banned from Internet cafes. Operating licenses may be withdrawn and fines imposed if these regulations are not properly implemented.

Internet Publishing Provision

On August 1, 2002, the following publishing regulations were passed. Article 6 : Engaging in Internet publishing activities may only be done through permission. No unit or individual may engage in Internet publishing activities without permission. No group or individual may interfere with, hinder or disrupt Internet publishing entities in engaging in Internet publishing activities in accordance with the law.

**i.e. In China there is no "free" communication on the Internet, as every posting is considered "publishing".*

Bulletin Board Provisions

Starting on November 11, 2002, the following articles came into effect. *Article 5:* Operators of Internet Information Services who also establish electronic bulletin board services shall, when applying to the provincial, autonomous region, or independent municipality telecommunications administration agency, or the Ministry of Information Industry for a Commercial Internet Information Service License or undertaking registration as a non-commercial Internet Information Service, set forth this fact specifically in their application or registration.

Article 11: Electronic bulletin board providers shall provide only services in accordance with the category or subject matter areas that have been permitted, and may not provide services that exceed these categories or establish other subject matter areas.

Article 13: If an electronic bulletin board provider notices that any information falling under Article 9 of these regulations has appeared on its electronic bulletin board service system, they shall immediately delete it, retain the relevant records, and report it to the relevant authorities.

**i.e. Operators of BBSs must monitor the content and suppress anything that goes against anything the government doesn't like—or risk being shut down, which they often are.*

Surveillance Software Mandated in Internet Cafes

On September 29, 2002, regulations on Internet Cafes were passed. *Article 23:* Units operating Internet Access Service Business Establishments shall examine, register, and keep a record of the identification card or other effective document of those customers who go online. The contents of the registration and records shall be maintained for at least 60 days, and shall be provided to the cultural and public security agencies for examination in accordance with the law. Registration contents and records shall not be altered or destroyed during this period.

**i.e. Internet cafes are required to keep personal information on internet users. They must also monitor what pages users are accessing. Internet cafes are being used as internet police for government.*

In October 2003, the Ministry of Culture announced that by the year 2005 all China's 110,000 Internet cafes will need to install surveillance software which would be standardized throughout all Internet cafes in China. The Ministry of Culture also intends to issue licenses to allow up to 100 companies to manage the majority of Internet cafes. "We are actively pushing an internet cafe technology management system requiring the whole nation to adopt the same standard and each province the same software" said Liu Yuzhu, an official from the Ministry of Culture. According to Liu Qiang, a senior official with the Ministry of Culture, the software would make it possible to collect personal data of Internet users, to store a record of all the web-pages visited and alert the authorities when unlawful content was viewed.

In November, the Ministry of Information Industry (MII) issued rules for approximately 30 large companies that manage Internet addresses in China. While these regulations appear to be intended to improve service standards, they are also aimed at strengthening control over sensitive information posted on the web. According to the MII, such firms must have "strict and effective mechanisms for cleaning bad and offensive domain names, which should be done once a day".

In December, Internet news and information providers, including Renmin, Xinhua, Sina, Sohu and Net Ease, signed up to a new "Internet News Information Service Self-Discipline Pledge". Signatories to the Pledge agree to "obey government administration and public supervision voluntarily, to resist firmly the Internet transmission of harmful information such as obscenity, pornography and superstition, and to resist the substance of information [sic] that violates the fine cultural traditions and moral codes of the Chinese nation".

The introduction of this Pledge echoes similar measures taken in March 2002, when a broader range of companies signed up to the "Public Pledge on Self-Discipline for the China Internet Industry". While Amnesty International recognizes the right of the authorities to regulate the Internet, the vague wording of such Pledges and the lack of definition of key concepts such as "harmful" and "super-

stitious" allows a wide degree of interpretation. Amnesty International is concerned that these Pledges will be used in conjunction with existing rules and regulations to restrict the fundamental freedom of Internet users to access information or express their views and opinions online.

IMPLEMENTING THE RESTRICTIONS

The Internet is a popular and powerful channel for the government and ordinary Chinese to hear each other and to be heard. However, the controls placed on operators and users of the Internet have increased greatly in recent years. This has taken the form of censorship and penalties against all those involved with bulletin boards, chat rooms, e-mail and search engines who contravene the provisions of the Criminal Law and the scores of regulations.

As all communication on the Internet in China passes through government-controlled routers the authorities are able to block access to many sites and to filter content and delete individual links or web pages if considered "dangerous" or "subversive". No list is publicly available on what is filtered and blocked, but a study done by the Harvard Law School on *Empirical Analysis of Internet Filtering in China*, carried out between May and November 2002 and updated on December 3, 2002, found that over 50,000 of 204,000 web sites tested were inaccessible from at least one location in China although some were accessible from the U.S.

1. Blocking

The authorities routinely block news sites, especially foreign-based sites, including those featuring dissident views or banned groups. The blocking appears to be intermittent but more prevalent at times of heightened security such as the anniversary of the crackdown on the 1989 pro-democracy protests, the annual meeting of the National Party Congress or visits from heads of state or government.

Many websites considered to contain politically sensitive information, such as those of human rights organizations and banned groups as well as international news sites, are inaccessible from China. Amnesty International's main website, along with hundreds of others, continues to be blocked. The average Internet user in China knows there are certain sites that are accessible, searches that cannot be done, or content that cannot be looked at.

In late August 2002, the popular search engine, Google.com, could not be accessed from China for several weeks. Altavista.com was also reportedly blocked. Protest messages were registered on bulletin boards throughout China. In hopes of capturing a larger market of Internet users, most foreign companies operating in China now avoid such confrontations by censoring their search engines (as do the Chinese). Such companies block specific websites on the request of the Chinese government.

2. Filtering

In mid-September 2002, China introduced new filtering systems based on key words, regardless of site or context. Automated technology blocks any communication in which certain banned words appear. Filtering software has reportedly been installed on the four main public access networks in China. Prohibited words or strings of words on websites, e-mail, personal blogs, foreign news sites and search engines are affected. Users trying to access information which includes key words such as 'Taiwan', 'Tibet', 'democracy', 'dissident', 'Falun Gong', 'Dalai Lama', and 'human rights', have continued to be regularly blocked. In addition, several new regulations have created greater responsibilities for control of the Internet through Internet cafes, companies and, most recently, portals providing news.

Filtering technology has largely been provided by Western internet companies, including U.S. based corporations. Among those providing filtering software are Cisco, Nortel Networks, Sun Microsystems, Juniper, and 3COM. Cisco has provided routers to China that can block not only entire websites, but also specific sub-pages, leaving the rest of the site accessible. Groups and individuals in China have used a variety of means to overcome Internet censorship including the use of proxy servers situated outside of China, which circumvent firewalls and the blocking of websites.

3. The Closure of Internet Cafes

Following a fire at Lanjisu Internet café in Beijing in June 2002 which killed 25 people, the Public Security Ministry announced that it had closed down 2,400 Internet cafes in Beijing for safety reasons. Officials in other cities such as Shanghai and Tianjin took similar action. Since then the authorities have introduced a range of regulations affecting Internet cafes, instituted government checks and ordered filtering software to be installed.

While Amnesty International recognizes the importance of health and safety regulations for all public services including Internet cafes, the organization is concerned that the fire at the Internet café in Beijing may have been used as a pretext to crackdown still further on freedom of expression in China.

According to a recent statement issued by the Minister of Culture, there are 200,000 Internet cafes throughout China but only about 110,000 of them are officially registered. All Internet café owners have been obliged this year to re-register with a number of different authorities to obtain a license and avoid being shut down or fined heavily.

Several weeks after the Beijing Internet café fire, the government ordered all Internet cafes to augment their filtering software within weeks and to keep records of all users for a 90-day period. The software prevents access to 500,000 foreign websites, such as foreign newspapers, Falun Gong websites, websites on democracy and human rights and others which are considered "reactionary" or are "politically-sensitive". Those attempting to access these banned sites are automatically reported to the Public Security Bureau. Internet police in cities such as Xi'an and Chongqing can reportedly trace the activities of the users without their knowledge and monitor their online activities by various technical means.

PUBLIC PLEDGE ON SELF-DISCIPLINE FOR CHINA INTERNET INDUSTRY

In addition to enforcing controls directly, the Chinese authorities are using a variety of means to force Internet companies to take greater responsibility for implementing the numerous laws and regulations controlling the use of the Internet in China. In March 2002, the Internet Society of China issued The Public Pledge on Self-Discipline which entered into force in August 2002.

Signatories to the Pledge agree to:

". . . Refrain from producing, posting or disseminating pernicious information that may jeopardize state security and disrupt social stability, contravene laws and regulations and spread superstition and obscenity."

Those concerned with the restrictions placed by the authorities on freedom of expression in China regard the Pledge as another means of censoring certain types of information disseminated on the Internet which is deemed to be politically sensitive.

In July 2002 the Pledge had been signed by over 300 signatories including the U.S.-based search engine Yahoo!. A lawyer working at Yahoo! reportedly stated that Yahoo! will conform to local laws in countries where it operates.

While Amnesty International recognizes that Internet companies should be regulated and that restrictions on their activities may be legitimate, AI is concerned at the wide-ranging and broadly defined nature of this Pledge. The organization fears that this new instrument will be used as part of wider attempts to restrict the freedom of expression and association of Internet users in China.

INTERNET FREEDOM AND CORPORATE RESPONSIBILITY

The rapid rise of the Internet has been greatly aided by the involvement of foreign companies in China. Foreign telecommunications, software and hardware companies are investing heavily in the development of China's Internet.

Amnesty International is concerned at reports that some foreign companies may be providing China with technology which is used to restrict fundamental freedoms.

Sohu.com, a Chinese Internet portal, reportedly funded by overseas companies, and financed by leading investment banks and other venture capital firms from the West, reminds those accessing its chat room that "topics which damage the reputation of the state" are forbidden. "If you are a Chinese national and willingly choose to break these laws, Sohu.com is legally obliged to report you to the Public Security Bureau".

In November 2000, the Ministry of Public Security launched its "Golden Shield" project. This project aims to use advanced information and communication technology to strengthen police control in China and a massive surveillance database system will reportedly provide access to records of every citizen. To realise this initiative, China depends on the technological expertise and investment of foreign companies.

Amnesty International remains concerned that in their pursuit of new and lucrative markets, foreign corporations may be indirectly contributing to human rights violations or at the very least failing to give adequate consideration to the human rights implications of their investments. In its first report on *State Control of the Internet in China*, Amnesty International cited Cisco Systems, Microsoft, Nortel Networks, Websense and Sun Microsystems as reportedly having provided technology which has been used to censor and control the use of the Internet in China.

Following the publication of this report, several companies dismissed allegations that their company's actions might be contributing to human rights violations in China. Cisco Systems denied that the company tailors its products for the Chinese market, saying that "[I]f the government of China wants to monitor the Internet, that's their business. We are basically politically neutral." Microsoft said it "focused on delivering the best technology to people throughout the world", but that it "cannot control the way it may ultimately be used."

Amnesty International considers such responses to be inadequate, particularly in view of recent measures taken at the international level to hold companies more accountable for the human rights implications of their investments. For example the UN Human Rights Norms for Business, adopted in August 2003, state that:

> [T]ransnational corporations and other business enterprises shall refrain from any activity which supports, solicits, or encourages States or any other entities to abuse human rights. They shall further seek to ensure that the goods and services they provide will not be used to abuse human rights.

In November 2005, Amnesty International contacted Microsoft and Yahoo! regarding these issues. We urged both companies to conduct their business in China, as elsewhere, in a manner that respects human rights, abides by international human rights standards and avoids complicity in human rights violations. The Internet providers' argument that they are "bringing the Internet to China" is outdated and unacceptable. The Internet already is in China, and such justification should no longer be used when defending their actions. Amnesty International urges all companies which have provided such technology to China to use their contacts and influence with the Chinese authorities to bring an end to restrictions on freedom of expression and information on the Internet and to urge the release of all those detained for Internet-related offences in violation of their fundamental human rights.

DECLARATION OF CITIZENS' RIGHTS FOR THE INTERNET

In protest against the measures taken by the authorities to control freedom of expression and freedom of information and association on the Internet, a group of 18 dissidents and intellectuals published a *Declaration of Citizens' Rights for the Internet* on July 29, 2002.

This Declaration challenges the regulations introduced by the authorities and urges the National People's Congress and international human rights organizations to examine the constitutionality and legitimacy of certain regulations. By October 2002 the Declaration had the support of over 1000 web publishers and Internet users.

The Declaration cites the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights and states that,

> *". . . a modern government should be based on the right of individual freedom of speech, the right of organizing associations, the right of questioning government decisions and the right of openly criticizing the government.*
>
> *. . . A modern society should be an open society. At the historical juncture of the Chinese nation once again transforming itself from a traditional society to a modern society, any blockade measures are all unfavourable to China's society joining paths with the world and the peace and progress of China's society.*
>
> *. . . Every citizen and government should undertake its responsibility and it has become extremely urgent to safeguard Internet freedom."*

One of its signatories, Wan Yanhai, a doctor and web site publisher, was detained on August 25, 2002 on suspicion of "leaking state secrets" and released on September 20, 2002 following international campaigning on his behalf by human rights organizations. He was arrested in connection with publishing a document on the internet detailing deaths from AIDS in Henan Province as a result of selling blood to government-sanctioned blood collectors.

Wan Yanhai worked at the AIDS Action Project, a Beijing-based education and activism group, whose offices were closed by the authorities in June 2002. The web site, (*www.aizhi.org*) an important independent source of information about the HIV/AIDS crisis in China, had promoted the rights of farmers in Henan Province who had contracted AIDS from selling blood.

On August 1, 2002, Wan Yanhai had circulated an online appeal to all independent Web publishers asking them to join him in protesting against new regulations by giving themselves up to the authorities for operating "illegal" websites. Wan Yanhai had also reportedly made use of Internet chat rooms, discussion and e-mail groups in his efforts to publicise his cause and promote freedom of opinion and expression in China.

Despite the measures introduced by the authorities to stifle freedom of expression over the Internet, the new technology is a cornerstone for economic growth in a country with over a fifth of the world's population. As the importance of the Internet grows so too will the millions of users and the demands of those seeking justice and respect for human rights in China.

PRECEDENT FOR STATE DEPARTMENT SUPPORT OF VOLUNTARY INDUSTRY INITIATIVES

Among our recommendations for the U.S. Government is support (including funding) for an industry-wide voluntary initiative to develop standards for the IT sector as regards human rights. The Government is in a position to support such a voluntary initiative, given the growing presence of U.S.-based IT companies overseas. There is precedent for this type of support by the U.S. Government, including the Voluntary Principles for Security and Human Rights for the extractive industry and the Apparel Industry Partnership, formed on the initiative of President Clinton, which has since grown into the Fair Labor Association.

CONCLUSION AND RECOMMENDATIONS

In conclusion, we feel strongly that the willing submission of U.S. companies to Chinese practices of censorship and related human rights abuses in China presents a challenge which must be faced head on and fast by companies, the U.S. Government and the Chinese Government, in close consultation with NGOs such as Amnesty International.

Amnesty International urges President Bush to:

- Make his position clear on the internet companies' involvement in colluding with the Chinese Government in the Chinese Government's abuse of its citizens. The President should make a public statement condemning China's behavior and the cooperation of IT companies.
- To publicly raise US concern about the crackdown on Internet users in China, during his meeting with the Chinese President Hu's State visit to the Unites States in April.
- Get a commitment from President Hu on specific benchmarks to improve human rights in China, in the run-up to the Olympics in 2008.

Amnesty International urges Secretary Rice to:

- Make public any assistance the United States Embassy in China offered to IT companies in promoting their businesses in China.
- Make public any issues that were raised with the IT companies about their complicity with the Chinese Government in abusing Chinese citizens' human rights.
- Make public any interventions made with the Chinese Government about these abuses.
- Support an industry-wide voluntary initiative for the IT sector, to develop global standards on human rights. The process should be open and transparent and include stakeholders from business, governments and NGOs, and should lead to not only a set of principles, but explicit guidelines for implementation and evaluation.

Amnesty International calls on the Congress to:

- Initiate a study to fully examine U.S.-based multinational Internet technology corporations' activities overseas.
- Pass legislation regulating U.S. Internet technology companies operating overseas, and other companies publicly traded on U.S. stock exchanges (which would include Baidu, the primary Chinese competitor), requiring them to report on their participation in government-ordered filtering/censorship wherever they operate and prohibiting them from complying with violations of freedom of expression and information by repressive regimes.
- Contact Yahoo! directly, inquiring about the Shi Tao case and Yahoo!'s complicity with China's brutal repression of peaceful political speech.

Amnesty International calls on U.S. companies to:

- Use their contacts and influence with the Chinese authorities to bring an end to restrictions on freedom of expression and information on the Internet and to urge the release of Shi Tao and all those detained for Internet-related offenses in violation of their fundamental human rights.

- Take immediate steps to ensure that all their units—the parent corporation and subsidiaries—stop any actions that could undermine human rights in any country in which they operate, and uphold human rights responsibilities for companies as outlined by the UN Norms for Business.
- Develop an explicit human rights policy, ensuring that it complies with the UN Norms for Business.
- Participate in an industry-wide multi-stakeholder process to develop global principles on IT and human rights, which is open and transparent and includes NGO representatives, and that leads not only to a set of principles, but explicit guidelines for implementation and evaluation.
- Disclose any and all information about filtering/censorship occurring around the world

Amnesty International calls on the Chinese Government to:

- Allow freedom of expression, including on the Internet.
- Release Shi Tao and other Internet dissidents immediately and unconditionally.
- Set a time table to improve human rights in the run-up to the Beijing Olympics in 2008.

Thank you for inviting Amnesty International to testify at this important and timely hearing.

STATEMENT SUBMITTED FOR THE RECORD BY MS. ANN COOPER, EXECUTIVE DIRECTOR, COMMITTEE TO PROTECT JOURNALISTS

CHINA, THE INTERNET, AND U.S. CORPORATE RESPONSIBILITY: PRINCIPLES BEFORE PROFITS

Mr. Chairman, thank you for allowing the Committee to Protect Journalists to present this testimony. CPJ, which celebrates its 25th anniversary this year, responds to attacks on the press worldwide. It documents more than 400 cases every year and takes action on behalf of journalists and their news organizations, without regard to political ideology. CPJ accepts no government funding and depends entirely on the support of foundations, corporations and individuals.

In the last year alone, the CPJ has documented Internet censorship in 22 countries, including Tunisia, Iran, Vietnam, and Nepal. Yet none raises as much concern as China, where the government has imprisoned at least 18 Internet writers. Our great fear is that China's authoritarian approach—aided by U.S.-based Internet companies—will become the model for repressive regimes wishing to restrict the flow of information.

Shi Tao, 37, an Internet essayist and former editor of the Changsha-based newspaper *Dangdai Shang Bao*, is among those imprisoned in China. He is serving a 10-year sentence for "leaking state secrets abroad" in a 2004 e-mail sent to the editor of an overseas Web site. The message described government instructions on how his newspaper should cover the 15th anniversary of the military crackdown on pro-democracy demonstrators in Tiananmen Square. The U.S.-based Internet company Yahoo helped Chinese authorities identify Shi through his e-mail account.

Shi's imprisonment is among several abuses in China aided by the commercially driven decisions of U.S.-based companies. "Do no evil" Google opted for the lesser of two evils and started censoring search responses in China. To soften the blow, Google tells Internet users behind China's firewall that more responses are available—they just cannot read them on Google.cn.

Microsoft has said it will abide by China's demands to shut down offending blogs. Under fire in the West, Microsoft has pledged that it will block access to material only within China or other countries where it is deemed unlawful, but will still make the sites available to outside users. The change in policy is a first response to the criticism Microsoft received for shutting down the site of Chinese blogger Zhao Jing, also known as Michael Anti.

Cisco Systems, which supplies much of the hardware that forms the World Wide Web, flatly denies that it has supplied China with the equipment and technology to control what the country's 100 million Internet users view online. Cisco's routers and other backbone equipment direct the digital flow of information over the Web and are integral to China's information firewall. Cisco says it has done no more than sell China the same equipment that it sells elsewhere in the world, and cannot stop China from adapting the equipment to its own needs. But skeptics question

Cisco's claims, saying that the technical support the company supplies with the equipment could easily be helping Chinese technicians to effectively censor the Web.

How to confront this problem before it spreads further? In the short term, it is not realistic to expect significant improvement in China's behavior, but there are steps that would help change the way U.S.-based companies behave in such situations. We believe that because of their superior technology and market dominance, these companies have considerable leverage to resist the demands made by governments seeking to censor information or identify and persecute those who exercise their right to free expression.

First, make a commitment to transparency. Internet and technology companies should make public portions of any final agreement with governments requiring censorship or the loss of online anonymity.

Lobby as a group to resist government pressure. U.S.-based Internet companies successfully joined with international corporate clients to work out a compromise with the Chinese government to pull back stringent 1999 government restrictions on encrypting Internet traffic. Encryption laws are still tighter in China than elsewhere, but they are not as limiting as first proposed. The industry then was motivated by the desire to protect commercial transactions and money transfers. A similar industry-wide effort should be organized around issues of censorship and identity protection.

Insist on transparent due process. The legal basis for censorship actions taken in China has been unclear. Companies that have acceded to China's demands have not said whether they were presented with a court order or merely instructed by a politician. In most democracies, prosecutors, courts, and complainants seek Internet companies' cooperation in a transparent manner guided by law. We urge companies to use the law in China and elsewhere to insist on due process.

If voluntary steps fail, legislation should be enacted. CPJ joins with other press freedom advocates in urging voluntary measures. If Chinese pressure on Internet companies to censor proves too strong, legislation would be in order to bar U.S.-based firms from exposing journalists to persecution or enabling government censorship. Legislation could level the playing field for all Internet companies, setting a uniform standard for corporate behavior on free expression issues.

U.S. technology and Internet companies are in demand in China because they offer superior products and services not readily available elsewhere. This is precisely what gives these companies leverage to resist Chinese government pressure and defend the basic human rights of their users. This is not a balancing test, in which companies weigh concern for human rights with their obligation to shareholders. If U.S.-based Internet companies are able to resist Chinese government pressure, in fact, it may help their bottom line because Chinese consumers would be attracted to their commitment to privacy.

Regardless, we agree with Human Rights Watch that if the condition for doing business in China is an agreement to censor political speech or turn over e-mails from dissidents when requested by authorities, then these companies should not operate there. The moral principles at stake are not negotiable.

BACKGROUND: CHINA'S ATTEMPTS TO CONTROL THE INTERNET

President Hu Jintao consolidated his leadership in March 2005 during a legislative session that formalized the transition of power from Jiang Zemin. Hu's administration has distinguished itself by its hard-line stance against dissidents, intellectuals, and activists, intensifying a far-reaching and severe crackdown on the media. In 2005, central authorities arrested and prosecuted journalists under broad national security legislation, while simultaneously ramping up the regulations that undermine the right to express opinions and transmit information in China.

The government's ambitious project of media control is unique. Never have so many lines of communication in the hands of so many people been met with such obsessive resistance from a central authority. The Chinese government has merged its participation in the world market and political affairs with a throwback attachment to Mao-era principles of propaganda. By fostering technological and commercial growth, it has placed the media in the hands of ordinary citizens—and then used these same capabilities to block its citizens from blogging the word "democracy," publishing an independent analysis of relations with Taiwan, sending a text message about a protest, or reporting on the workings of the Propaganda Department.

More people use cell phones in China than anywhere else in the world, even as authorities continue to monitor and censor text messages. The nation's Internet users surpass 100 million by most estimates, although they face a massive and sophisticated government firewall restricting news and information.

In September 2005, the government announced a fresh set of restrictions on Internet news content that seemed to reflect its concerns over anti-Japanese demonstrations and increasingly frequent rural protests in 2005. The rules added two new areas of forbidden content to a list that already included news that "divulges state secrets," "jeopardizes the integrity of the nation's unity," "harms the honor or interests of the nation," or "propagates evil cults" (an apparent reference to the banned Falun Gong religious sect). The new regulations also banned content that incites "illegal" gatherings or demonstrations, or is distributed in the name of "illegal civil organizations." Web sites posting restricted news content would be fined or shut down, according to the regulations.

The new Internet restrictions also aimed to stem independent reporting and commentary by requiring bulletin board systems, Web sites associated with search engines, and online text messaging services to register as news organizations. The rules stated that Web sites that had not been established by an official news outlet ("news work unit") were forbidden from gathering or editing their own news or commentary. The regulations outlawed the kind of self-generated news and commentary that had become a fixture of search portals like *Sina* and *Sohu* and popular bulletin board systems such as *Xici Hutong*. Administrators of these sites had long censored their own news content and monitored public discussions to avoid being shut down by authorities, but the new restrictions added a layer of direct government involvement in their practices while limiting their legitimate scope.

Less than a week after these regulations were issued, the popular bulletin board system *Yannan* posted a notice that it would be closed for "cleanup and rectification" until further notice. The Web site's administrators had earlier deleted all entries related to the turbulent recall campaign in the village of Taishi, which pitted hundreds of protesting villagers against local officials and police. The Taishi protests captivated observers around the country, who saw it as a test of the government's commitment to experiments in "grassroots" democracy. *Yannan* was pivotal in providing updated information and commentary that went further in scope and diversity of opinion than the restricted coverage allowed in mainland print and broadcast news.

It seems unlikely that the Chinese government will curtail its efforts to control and suppress information in the near future. In a superficial way, authorities are meeting with success in controlling dissent. But many journalists, writers and activists in China are dedicated to getting information out via the Internet when they are frustrated by censored, state-sanctioned news outlets. Their passion for the truth keeps journalism alive.

Couple that journalistic desire with the increasing competitive pressures to produce stories that grab readers' attention and meet those readers' rising expectations for accurate and timely information, and you have a potent formula for change. It seems reasonable to assume that Chinese journalists will continue to push against the barriers the government throws in front of them.

The Committee to Protect Journalists continues to watch as growing numbers of Chinese reporters, driven by their own passion and aided by the Internet, turn themselves from state propaganda workers into solid news reporters in the best tradition of journalism. That is a trend that we think is sure to continue in China.

JAILED: INTERNET WRITERS BEING HELD IN CHINA

According to CPJ research, China was the world's leading jailer of journalists for the seventh consecutive year in 2005, with 32 behind bars on December 1. Around half of those were Internet journalists. The following are writers and journalists who remained in prison late last year for disseminating information online.

Wu Yilong, *Zaiye Dang*
Imprisoned: April 26, 1999
Mao Qingxiang, *Zaiye Dang*
Imprisoned: June 1999
Zhu Yufu, *Zaiye Dang*
Imprisoned: September 1999

Wu, an organizer for the banned China Democracy Party (CDP), was detained by police in Guangzhou on April 26, 1999. In June, near the 10th anniversary of the brutal crackdown on pro-democracy demonstrations in Tiananmen Square, authorities detained CDP activist Mao. Zhu, also a leading CDP activist, was detained in September. The three were later charged with subversion for, among other things, establishing a magazine called Zaiye Dang (Opposition Party) and circulating pro-democracy writings online. On November 9, 1999, all the journalists were convicted of subversion. Wu was sentenced to 11 years in prison. Mao was sentenced to eight years, and Zhu to seven years.

Yang Zili, *Yangzi de Sixiang Jiayuan*
Xu Wei, *Xiaofei Ribao*
Jin Haike, freelance
Zhang Honghai, freelance
Imprisoned: March 13, 2001

Yang, Xu, Jin, and Zhang were detained on March 13 and charged with subversion on April 20. On May 29, 2003, the Beijing Intermediate Court sentenced Xu and Jin to 10 years in prison each on subversion charges, while Yang and Zhang were sentenced to eight years each on similar charges.

The four were active participants in the Xin Qingnian Xuehui (New Youth Study Group), an informal gathering of individuals who explored topics related to political and social reform and used the Internet to circulate relevant articles. Yang, the group's most prominent member, published a Web site, *Yangzi de Sixiang Jiayuan* (Yangzi's Garden of Ideas), which featured poems, essays, and reports by various authors on subjects such as the shortcomings of rural elections. Authorities closed the site after Yang's arrest.

Tao Haidong, freelance
Imprisoned: July 9, 2002

Tao, an Internet essayist and pro-democracy activist, was arrested in Urumqi, the capital of the Xinjiang Uighur Autonomous Region (XUAR), and charged with "incitement to subvert state power." According to the Minzhu Luntan (Democracy Forum) Web site, which had published Tao's recent writing, his articles focused on political and legal reform. In one essay, titled "Strategies for China's Social Reforms," Tao wrote that "the Chinese Communist Party and democracy activists throughout society should unite to push forward China's freedom and democratic development or else stand condemned through the ages."

In early January 2003, the Urumqi Intermediate Court sentenced Tao to seven years in prison. His appeal to the XUAR Higher Court later in 2003 was rejected.

Abdulghani Memetemin, East Turkistan Information Center
Imprisoned: July 26, 2002

Memetemin, a writer, teacher, and translator who had actively advocated for the Uighur ethnic group in the northwestern Xinjiang Uighur Autonomous Region, was detained in Kashgar, a city in Xinjiang, on charges of "leaking state secrets."

In June 2003, Kashgar Intermediate People's Court sentenced him to nine years in prison, plus a three-year suspension of political rights. Radio Free Asia provided CPJ with court documents listing 18 specific counts against Memetemin, including translating state news articles into Chinese from Uighur; forwarding official speeches to the Germany-based East Turkistan Information Center (ETIC), a news outlet that advocates for an independent state for the Uighur ethnic group; and conducting original reporting for the center. The court also accused him of recruiting additional reporters for ETIC, which is banned in China.

Cai Lujun, freelance
Imprisoned: February 21, 2003

Cai was arrested at his home in Shijiazhuang, Hebei province. In October 2003, the Shijiazhuang Intermediate People's Court sentenced him to three years in prison on subversion charges.

Cai, 35, had used pen names to write numerous essays distributed online calling for political reforms. His articles included "Political Democracy Is the Means; A Powerful Country and Prosperous Citizenry Is the Goal"; "An Outline for Building and Governing the Country"; and "The Course of Chinese Democracy."

Luo Changfu, freelance
Imprisoned: March 13, 2003

Public security officials arrested Luo at his home in Chongqing municipality and charged him with "subversion." On November 6, 2003, the Chongqing No. 1 Intermediate Court sentenced him to three years in prison.

Luo, 40, is an unemployed factory worker. Before his arrest, he had actively campaigned for the release of Internet essayist Liu Di, who was arrested in November 2002 and released on bail a year later. Luo had written a series of articles calling for Liu's release and protesting the Chinese government's censorship of online speech. His essays also called for political reforms in China.

Luo Yongzhong, freelance
Imprisoned: June 14, 2003

Luo, who has written numerous articles that have been distributed online, was detained in Changchun, Jilin province. On October 14, the Changchun Intermediate

Court sentenced him to three years in prison and two years without political rights upon his release, which is scheduled for June 13, 2006.

In sentencing papers, which have been widely distributed online, the court stated that between May and June 2003, Luo wrote several essays that "attacked the socialist system, incited to subvert state power, and created a negative influence on society." Several specific articles were cited as evidence, including "At Last We See the Danger of the Three Represents!"—a reference to a political theory formulated by former President Jiang Zemin—and "Tell Today's Youth the Truth about June 4," a reference to the military crackdown on peaceful pro-democracy protesters in June 1989. According to the court papers, the articles were published on online forums including *Shuijing Luntan* (Crystal) Web site.

Luo has also written a number of articles advocating the rights of people with disabilities.

Huang Jinqiu, *Boxun News*
Imprisoned: September 13, 2003

Huang, a columnist for the U.S.-based dissident news Web site *Boxun News*, was arrested in Jiangsu province. The Changzhou Intermediate People's Court sentenced him on September 27, 2004, to 12 years in prison on charges of "subversion of state power," plus four years' deprivation of political rights.

Huang worked as a writer and editor in his native Shandong province, as well as in Guangdong province, before leaving China in 2000 to study journalism in Malaysia. While he was overseas, Huang began writing political commentary for *Boxun News* under the pen name "Qing Shuijun." He also wrote articles on arts and entertainment under the name "Huang Jin." In January 2003, Huang wrote in his online column that he intended to form a new opposition party, the China Patriot Democracy Party. When he returned to China in August 2003, he eluded public security agents just long enough to visit his family in Shandong province. In the last article he posted on *Boxun News*, titled "Me and My Public Security Friends," Huang described being followed and harassed by security agents.

Kong Youping, freelance
Imprisoned: December 13, 2003

Kong, an essayist and poet, was arrested in Anshan, Liaoning province. He had written articles online that supported democratic reforms and called for a reversal of the government's "counterrevolutionary" ruling on the pro-democracy demonstrations of 1989, according to the Hong Kong-based Information Center for Human Rights and Democracy.

Kong's essays included an appeal to democracy activists in China that stated, "In order to work well for democracy, we need a well-organized, strong, powerful, and effective organization. Otherwise, a mainland democracy movement will accomplish nothing." Several of his articles and poems were posted on the *Minzhu Luntan* (Democracy Forum) Web site. On September 16, 2004, the Shenyang Intermediate People's Court sentenced Kong to 15 years in prison.

Shi Tao, freelance
Imprisoned: November 24, 2004

Officials from the Changsha security bureau detained Shi near his home in Taiyuan, Shanxi province, on November 24, 2004, several months after he e-mailed notes detailing the propaganda department's instructions to the media about coverage of the anniversary of the crackdown at Tiananmen Square. On December 14, authorities issued a formal arrest order, charging Shi with "leaking state secrets." On April 27, 2005, the Changsha Intermediate People's Court found Shi guilty and sentenced him to a 10-year prison term.

Shi's verdict, which was leaked to the public, revealed that the U.S.-based Internet company Yahoo had given Chinese authorities information about Shi's e-mail account that was used to convict him.

In November 2005, CPJ honored Shi with its annual International Press Freedom Award for his commitment to free expression.

Zheng Yichun, freelance
Imprisoned: December 3, 2004

Zheng, a former professor, was a regular contributor to overseas online news sites including *Dajiyuan* (Epoch Times). He wrote critically about the Communist Party and its control of the media. He was imprisoned in Yingkou, in Liaoning province. On September 20, Zheng was sentenced to seven years in prison, to be followed by three years' deprivation of political rights, for "inciting subversion."

Prosecutors cited dozens of articles written by the journalist, and listed the titles of several essays in which he called for political reform, increased capitalism in China, and an end to the practice of imprisoning writers.

Sources familiar with the case believe that Zheng's harsh sentence may be linked to Chinese leaders' objections to the *Dajiyuan* series "Nine Commentaries on the Communist Party," a widely read and controversial look at Chinese Communist Party history and current practices.

Zhang Lin, freelance
Imprisoned: January 29, 2005

Zhang, a political essayist and dissident who wrote regularly for overseas online news sites, was detained on his return to Bengbu in central China's Anhui province after traveling to Beijing to mourn the death of Zhao Ziyang, the ousted general secretary of the Communist Party. On March 19, 2005, Zhang's wife Fang Caofang received notice that he had been formally arrested on allegations of inciting subversion.

Zhang's lawyers argued that the six articles and one radio interview cited by the prosecution, in which he criticized the Communist Party and the Chinese government, were protected free expression. Zhang's wife believes that his imprisonment is also connected to essays he wrote about protests by unemployed workers and official scandals, according to Agence France-Presse.

On July 28, the court convicted Zhang and sentenced him to five years in prison. Zhang's appeals were rejected twice. He is detained at Bengbu No. 1 Detention Center. In September, Zhang waged the hunger strike for 28 days to protest his unjust sentence and the harsh conditions of his detention center.

Li Jianping, freelance
Imprisoned: May 27, 2005

Authorities detained Li on May 27 in Zibo, a city in northeastern China's Shandong province, and formally arrested him for defamation on June 30, according to *ChinaEForum*, a U.S.-based dissident news forum.

Li wrote frequently for overseas news Web sites banned in China, such as *Boxun News, Epoch Times, China Democracy* and *ChinaEWeekly*. Some of his articles directly criticized Chinese Communist Party leadership, including former and current Chinese presidents Jiang Zemin and Hu Jintao. Just days before his detention, Li wrote a strongly critical analysis of Hu Jintao's policy toward Taiwan, posted on ChinaEWeekly on May 17. It was unclear which of his articles led to his detention.

In August, Li was formally indicted on charges of inciting subversion.

THE INTERNET IN CHINA: A TOOL FOR FREEDOM OR SUPPRESSION?

Testimony before the House Committee on International Relations
Subcommittee on Africa, Global Human Rights & International Operations
February 15, 2006

By Lance M. Cottrell, Global Privacy Advocate
Founder and Chief Scientist
Anonymizer, Inc.

Honorable Chairman Christopher Smith,
Distinguished Members of the Subcommittee,

I am honored to be invited to share my insight on the current state of China's censorship of their citizens' Internet usage. I would like to express my gratitude for being able to provide the details of a new solution that Anonymizer is developing to provide the People's Republic of China with uncensored access to the Internet. I will also briefly explain why Anonymizer has chosen to provide this solution to China for free. Finally, I will comment on Reporters Without Borders proposal and add my perspective on legislative decisions.

ANONYMIZER'S ANTI-CENSORSHIP SOLUTION

Anonymizer is currently developing a new anti-censorship solution that will enable Chinese citizens to safely access the *entire* World Wide Web filter-free, while free from oppression and fear of persecution or retribution. This new program expands upon Anonymizer's history of human rights efforts which provide a censor-free, safe Internet experience for those in oppressed nations.

This new anti-censorship solution will be available to Chinese citizens before quarter's end. The solution will provide a regularly changing access point that enables users to open the unobstructed doors of the World Wide Web. In addition, the users' identities will be protected from online tracking and monitoring by the Chinese government.

Interested Chinese citizens will be able to submit their email address either through a Web page or via dissidents outside of the great firewall of China. Once added to Anonymizer's mailing list, the recipient will receive a daily email that includes a link to download the anti-censorship software, as well as updated configuration for the program. Both of these items will change daily to stay one step ahead of the Chinese government and to avoid blocking. This email list will be protected within Anonymizer's secure networks and will not be shared, rented, or sold to any third party.

The software will make a secure (SSL) connection to Anonymizer's anti-censorship servers through a frequently changing set of IP addresses that are not associated with

Anonymizer. From there, the user's connection will continue to its destination over the uncensored Internet, and will appear to come from yet another IP address. This system will ensure that the user is protected both from interception and blocking of their Internet traffic when exiting China. It will also protect against monitoring of forums or other Web sites which will try to detect the users IP address within China.

Any attempt to monitor this connection from within China will only see ordinary SSL Web connections to uncontroversial domains. Any monitoring of IP addresses accessing forums, Web-mail sites, blogs, or discussion boards will show Anonymizer IP addresses which are impossible to track back to the originating IP address.

Anonymizer's solutions are all designed to make it impossible to track connections back to identify the user of the system.

FREE SERVICE FOR CHINA

There are many US companies that do not respect freedom of expression when operating in repressive countries. Unfortunately, companies such as Google, Cisco, Yahoo!, and Microsoft are reaping financial gains at the expense of those under the thumb of repressive regimes. In addition to this, the practices of these U.S.-based companies are tarnishing the image of America abroad.

Anonymizer is not willing to sit idly by while the freedom of the Internet is slowly crushed. Because of this, the company decided to provide this anti-censorship solution to the People's Republic of China for free.

Anonymizer is providing this solution in part to prove that the choice of "capitulate or lose" is a false dichotomy. By leveraging the appropriate technology, a company can achieve access without sacrificing its principles. Any of these collaborating companies could use anti-censorship technologies similar to Anonymizer's to ensure that their content and services would be available within oppressed countries without having to facilitate the oppression in any way. Although there would be some cost in providing this service, as there is to Anonymizer, profits can not be the only factor in driving corporate decision making.

LEGISLATION

Current anti-bribery laws set a precedent for regulating U.S. companies operating within other countries. Although these laws put American companies at a slight disadvantage in the global economy, they were established to set a standard of conduct by which all U.S. must companies abide. It was simply the right thing to do.

The U.S. government also restricts exports of certain munitions to specified countries. Although these countries may still be able to obtain the munitions, it is simply not appropriate for U.S. companies to aid our military opponents.

Similarly, it is imperative for U.S. companies to take more responsibility for their actions in repressed countries with filtering and Internet surveillance technologies. I believe that

U.S. companies should not aid and abet these repressive regimes in the suppression of their people.

While I question whether the details of the Reporters Without Borders proposal are realistic, I strongly endorse the idea and principles behind their request for a code of conduct. Therefore, I recommend that the Committee formally request a code of conduct without mandating the specific logistical details requested by RSF. Let these technology experts determine the right thing to do.

In addition, it is practically impossible for a small handful of companies to effectively create a code of conduct that all companies must follow. I would encourage a large panel of companies from several industries to participate, thus ensuring a complete and obtainable code of conduct that all companies will embrace.

It takes tremendous strength of will and character for a company to take a principled stand on its own, while its competitors reap the benefits of collaboration with the oppressors. Only with wide spread adoption of a code of conduct, either voluntary or legislated, will we see the individual cost to a company become manageable.

It is not enough for only U.S. companies to take this stand. The Internet is far too global, with most major players having presence distributed throughout the world. A unified front is necessary not just in the United States but internationally as well. To ensure success, it is critical to gain the support of our global partners, including the Organization for Economic Co-operation and Development and the United Nations.

CONCLUSION

The communist government in China has taken a hard line against freedom of the press and access to information on the Internet. Google and others have been forced into a box by the Chinese government's strict requirements, but Anonymizer stands firm on the issue of protecting civil liberties. The company has been protecting these basic rights for more than a decade and we are poised to help the people of China as well.

Mr. Chairman, we urge you to formally request the leading technology companies to develop a code of conduct that we can all stand behind. As global leaders, we must take responsibility for our actions, or in this case, transactions. Everyone is worthy of these basic human rights and our companies should not profit at the expense of others less fortunate.

The team at Anonymizer is thrilled to be able to develop and provide this new solution to the people of China. We believe we are turning on a light in a world of near-darkness. Help us educated them on democracy, Tiananmen Square, civil rights, and freedom of expression. The Internet has always had the potential to make the world a better place. Lets us ensure that it is able to live up to that potential rather than becoming a tool of oppression and propaganda.

JOINT INVESTOR STATEMENT ON FREEDOM OF EXPRESSION AND THE INTERNET

RELEASED NOVEMBER 7, 2005 AT THE OVERSEAS PRESS CLUB NY,NY

As investors and research analysts, we recognize that our investment decisions have an impact on human rights around the world. We are therefore committed to using the tools at our disposal to uphold human rights world wide as outlined in the United Nations Universal Declaration of Human Rights (UDHR), including freedom of opinion and expression, freedom of assembly and association, and security of persons.

The growth of the Internet offers considerable opportunities for global broad-based wealth creation. Companies involved in providing Internet services and technology are playing a leading role in building global communities and sharing knowledge. We believe that government action to censor, monitor, isolate and jail Internet users for exercising basic human rights outlined in the UDHR threatens the ultimate realization of these benefits. We believe these actions also present significant barriers to growth for Internet sector businesses, which depend on a broadly connected, free Internet.

To help advance freedom of expression, the undersigned:

- Reaffirm that freedom of expression is a universal human right that companies have an obligation to respect throughout their worldwide operations, and, in particular, in countries with a history of serious and widespread human rights violations;
- Reaffirm that Internet sector businesses have a particular responsibility in this domain for a number of reasons, including the following:
  - — Their long-term success depends on a broadly connected Internet that is free of censorship; and
  - — Millions of people depend on their products and services for reliable access to news and information;
- Recognize that, according to numerous and credible sources, a number of countries throughout the world do not tolerate public dissent and monitor and control citizens' access to the Internet as a means of suppressing freedom of expression;
- Recognize that some businesses help authorities in repressive countries to censor and mount surveillance of the Internet, and others turn a blind eye to the use made of their equipment;
- State that respect for freedom of expression is a factor we consider in assessing a company's social performance;
- Announce that we will monitor the operations of Internet businesses in repressive regime countries to evaluate their impact on access to news and information;
- Commit ourselves to supporting, at annual general meetings of publicly listed companies, shareholder resolutions that we believe are favorable to freedom of expression or otherwise promote the principles of this declaration;
- Call on Internet businesses to adopt and make public ethical codes stressing their commitment to freedom of expression and defining their obligations to uphold these freedoms, and
- Call on Internet businesses to make information public that will allow investors to assess how each firm is acting to ensure that its products and services are not being used to commit human rights violations (including, products and services that enable Internet censorship, surveillance and identification of dissidents).

Signatories representing over $22 billion USD in assets under management (as of Feb. 2006):

Boston Common Asset Management LLC
Domini Social Investments LLC
Trillium Asset Management
Walden Asset Management
Citizens Advisers, Inc.
Calvert Group, Ltd.
The Ethical Funds Company
Fondation Ethos
Bâtirente
Conscious Investors Pty Ltd
GES Investment Services

Harrington Investments, Inc.
Joyce Moore Financial Services
NorthStar Asset Management, Inc.
KLD Research & Analytics, Inc.
Jantzi Research Inc.
Ethibel
CorpGov.net
As You Sow Foundation
MMA
Dominican Sisters of Springfield, IL
Sisters of St. Francis of Philadelphia
Sisters of Charity of St Vincent de Paul of New York
Maryknoll Fathers and Brothers
Dominican Sisters of Hope
Mercy Investment Program
Sisters of Mercy Regional Community of Detroit
Ursuline Sisters of Tildonk-U.S. Province
Our Lady of Victory Missionary Sisters
Justice, Peace and Integrity of Creation Office, Missionary Oblates of Mary Immaculate, United States Province
Friends Fiduciary Corporation

STATEMENT SUBMITTED FOR THE RECORD BY BOSTON COMMON ASSET MANAGEMENT

Boston Common Asset Management LLC is a socially responsible investment firm that represents shareholders concerned with the long-term viability and social impact of corporations in which they may invest. Of particular interest to our shareholders, who hold millions of dollars worth of US technology stocks, is the assurance that their investment portfolios do not contribute to human rights abuses. While some corporate managers may contend that their cooperation with repressive regimes has been necessary in order to preserve shareholder value, our shareholders wish to be clear that they respectfully disagree. Boston Common Asset Management is here today to empower the progressive forces within our companies to avoid sacrificing the long-term business prospects promised by a free and broadly connected Internet for short term gains in repressive markets.

An open and borderless Internet provided the necessary opportunities for Cisco, Microsoft, Yahoo, and Google to grow into the successful, multibillion dollar businesses that sit before us today. To compromise the openness of the Internet is to weaken the foundation on which this value was built. Our shareholders recognize that the long-term growth and viability of Internet technology companies depends on the faith and perception of users that the Internet is open, reliable and secure. Internet traffic creates demand for IT infrastructure, network capabilities, and user platforms. As a result, growing volumes of Internet traffic unequivocally benefit businesses such as Cisco, Microsoft, Yahoo, and Google that profit from demand for these products and services. Any action by these companies that effectively reduces traffic, such as stifling the exchange of ideas or becoming a tool in political harassment campaigns, reduces demand for products and services these companies supply. Our shareholders support management in taking a principled stand on the issue of Internet freedom and human rights and in refusing to make this long-term sacrifice.

The U.S. State Department, among others, has documented a number of countries that engage in government action to censor, monitor, isolate and jail Internet users for exercising basic human rights. In China, Saudi Arabia, Vietnam, and Tunisia connectivity is growing, but the Internet that is developing is not open or secure. Management can no longer credibly assert that they are unaware of how their company's products and services may be used by the Chinese security apparatus. It is well documented that government authorities have consistently employed Internet technologies to help them violate basic human rights outlined in the 1948 United Nations Universal Declaration of Human Rights (UDHR), including freedom of opinion and expression (UDHR Article 19), security of persons (UDHR Article 3), privacy (UDHR Article 12), freedom of assembly and association (UDHR Article 20), and in many cases fair and impartial criminal hearings (UDHR Article 10). Through the use of censorship, surveillance, and threats of imprisonment Internet use is being actively discouraged by the Chinese government. In a number of instances these actions are undertaken with the complicity of US technology corporations. As shareholders we are discouraged by this short-sighted strategy. To aid a government intent on restricting Internet use, especially in a country that represents the largest

untapped market of users, undermines the profit maximization mission and ethical codes of conduct the companies before us today have agreed to uphold.

Our shareholders are concerned when management chooses to avoid today's uncomfortable confrontation and bows to repressive government clients at the expense of tomorrow's growth prospects and basic human freedoms. Pursuing sustainable corporate conduct allows management to choose the strategy most supportive of long-term shareholder value. Actions that serve to reduce the openness, safety and reliability of the Internet undoubtedly compromise the long-term business prospects of IT sector corporations. Engaging in short sighted business operations that undermine widely accepted human freedoms is simply not a sustainable practice. There is little excuse for such practice when it also reduces future business opportunity. Boston Common urges all the groups gathered here today to develop forward thinking, collaborative solutions that will encourage the sustainable, long term growth of IT sector companies and respect the basic human rights of all customers around the world. These goals should not be considered at odds with each other, but indeed dependent upon each other.

STATEMENT SUBMITTED FOR THE RECORD BY MS. PAM DIXON, EXECUTIVE DIRECTOR, WORLD PRIVACY FORUM

Chairman Smith, thank you for holding this hearing on the issue of China and the Internet. The World Privacy Forum has many questions about the role U.S. technology companies are playing in the Peoples' Republic of China (PRC). As you know, from infrastructure to search interfaces, U.S. companies such as Cisco, Microsoft, Google, and Yahoo are providing a variety of services in China. But the caveat is that some of these and other U.S. companies doing business in China have agreed to various terms set by the Chinese government, including censorship in some circumstances.

U.S. companies have frequently justified their cooperation with the Chinese government in part by citing a policy of engagement, arguing that increased information flow is the only way to bring increased freedom of information to China. While this argument may be defended in some circumstances, we must view the "engagement" argument as flawed as applied to the current configuration of U.S. technology deployment in China unless and until we are certain this engagement is not producing any harm to Chinese citizens.

Also flawed is the general opacity of U.S. technology corporations' operations in China. We know far less than we should about the practices and experiences of U.S. companies operating in China, and about their interactions with the Chinese authorities and Chinese customers. We do not have nearly enough information or facts on hand, but the scant information we do have is troubling. We know that Yahoo's operations in China have led to the arrest and jailing of at least one and possibly two Chinese citizens. We also know that Google is actively censoring Chinese searches at the request of the Chinese government.

The World Privacy Forum respectfully requests that Yahoo, Google, Microsoft, and other U.S. companies operating in the Peoples' Republic of China divulge the following information to Congress:

- The total number of PRC government requests of any type the companies have received while operating in China.
- The general nature and type of the PRC requests.
- The number of government requests for information about Chinese citizens.
- The number of government requests for information about American citizens and citizens of other countries.
- The number of PRC government requests U.S. companies have answered or fulfilled, and what kind of information has been turned over to Chinese authorities (categories of information).
- Answers to the question of what kind of notice is being given to Chinese citizens about the dangers and risks associated with the use of the technologies, especially Internet search and email tools. Specifically, copies of the privacy notices and safety warnings given to Chinese citizens who are using email and search technologies, including information about how prominent the warnings are and how simple or complex the wording of any warnings are, and statistics about how many Chinese users read the policies (or more correctly, visit the pages containing those policies).

- The total number of privacy-related inquiries sent to U.S. companies or their subsidiaries in China by Chinese customers of the companies, and ideally, the responses to those customer inquiries by the companies.

As citizens of a country with a democratic form of government, we have a deep responsibility to at the very least do no harm to citizens living under less free regimes. The issue of U.S. technology companies operating in countries with repressive regimes is not a new one—history has already given us the benefit of hindsight into similar matters from the past.

I do not cite the following example to make a direct historic comparison or to accuse current U.S. companies of creating a similar scenario, but rather to illustrate how crucial and how difficult it is for a company to be clear-sighted when dealing with other countries. In the 1930s IBM engaged with the Third Reich, primarily through its German subsidiary, Dehomag. IBM, through Dehomag, supplied its punch-card technology to assist the Third Reich with its 1933 census, the results of which were used to facilitate persecution of Jewish individuals, among others. The Holocaust would have occurred without IBM, but IBM technology did facilitate the goals of the Third Reich.[1]

There is no evidence that U.S. companies are aiding human misery on such a profound scale by establishing businesses in the Peoples' Republic of China. But IBM's lessons should nevertheless be considered carefully, particularly given that at least one Chinese citizen is in jail due to a U.S. company's involvement in and cooperation with the Peoples' Republic of China.

Let history judge us harshly if we do not ask the hard questions that we must about the role U.S. technology companies are playing in China today. It is our responsibility to get to the truth of what the impact of U.S. corporate involvement there has been, what it might be, and what it might mean. A dearth of knowledge and facts about this matter has hampered our full understanding of this issue. It is my hope that this hearing will mark the beginning of a long and robust process of putting facts forth and gaining real information and insight into the positives and negatives of U.S. corporate operations in China.

STATEMENT SUBMITTED FOR THE RECORD BY PETER YUAN LI, PH.D

I appreciate the opportunity to address the two committees on a topic of vital importance: the Internet in the People's Republic of China (PRC). I would like to discuss this problem and describe a powerful solution that is in place and, in fact, already underway.

I am a forty-one year old U.S. Citizen, and work as an information technology technician; my Ph.D in Electric Engineering is from Princeton University, and I am the holder of 20 patents. I am a devoted human rights activist and a practitioner of the Falun Gong spiritual discipline. I am also, as some of you might have seen in the news, a victim of the PRC's attempt to destroy internet freedom.

THE PROBLEM

My own experience of last week is telling. On February 8, agents of China stormed my house in Duluth, Georgia. The men, each Asian, were armed with knives and guns. They proceeded to bind me, gag me, and brutally beat me. They ransacked my house, taking two computers, my wallet, my home telephone, and files from a locked cabinet they broke open. While I lay bound on the floor, bleeding profusely, I heard another man arrive on the scene, who was apparently the group's leader; he spoke Chinese and demanded to know where my documents were kept. The men ignored valuables such as jewelry and other costly electronics.

This was not, by any stretch of the imagination, a random assault. These men and their means bear the unmistakable hand of the PRC, and characterize the alarming, disturbing lengths to which the communist regime in Beijing is willing to go to suppress freedom of information. I was attacked, you see, because I am actively involved in developing and maintaining Internet technologies that unblock PRC online censorship and enable Chinese internet users to securely exchange information and ideas without restrictions or threat of danger. The attack on me, it should be noted, is but one incident of many here in North America; the PRC has assaulted, spied on, threatened, and stolen the computers of several other Falun Gong Internet activists here in the democratic West.

It is a sad day when peaceful, law-abiding Americans like myself are not safe in their own homes from foreign dictatorships.

---

[1] See for example, Edwin Black's *IBM and the Holocaust*, Three Rivers Press, 2002.

Why, you might ask, would a regime such as China's go to such lengths as violent criminal assault on U.S. soil? The reason is simple: the regime fears more than anything else that the people of China will gain access to uncensored information, and it is persons like myself, in the free world, who are uniquely positioned to make this happen.

What might be hard to imagine is the unusual fear with which the PRC's unelected leader's rule. They are afraid that, if China's citizens gain access to uncensored news and information, they will learn about the untold crimes of the communist PRC regime, such as the Tiananmen Massacre of 1989; that they will learn about the leadership's corruption and cronyism; that they will learn about its darker activities, such as harvesting organs; and that perhaps, even, they will realize the United States is not a "evil hegemony" bent on destroying China. (Some of you might not realize that many Chinese persons, including those residing here in the U.S., celebrated both the 9–11 tragedy and the Columbia space shuttle disaster.) In a word, they fear that China's people will find out that they have been lied to. They fear that people will learn that there is a second side to the story. For the first time in 50-plus years of PRC rule, the people of China would be able to think through issues for themselves, and make informed decisions. China's people would have a taste of freedom of the press—an extraordinary thing, even if we can take it for granted in our lives. This would be, for one, immensely empowering to the people of China; and secondly, an important check on the Chinese Communist Party's (CCP) authoritarian rule.

In the PRC today, of course, there is very, very little freedom of the press. As you read this, a researcher for the New York Times is being held in a Chinese jail for the crime of reporting the truth. That New York Times reporter is but one of many Western journalists who have felt, first hand, the PRC's brutality against those who stand up for freedom of speech. The Internet has thus become the greatest hope for freedom of information in China; currently there are an estimated 110 million Internet users in China. While PRC authorities can easily shut down newspapers, ban books, confiscate documents, and incinerate hard-copy materials, the Internet is different. The internet is far more elusive. For this reason, China has deployed, according to The New York Times, some 50,000 so-called "cyber police," who are charged with monitoring Internet activity. Internet cafés must install video surveillance equipment and monitoring software, for example. Just attempting to visit a "banned" Website can get a person arrested; some have been sentenced to eight or more years in prison for sending one email that mentioned corruption by Communist Party officials. Additionally, China has built, as many of you know, a so-called "Golden Shield" online technology with which it censors information with consistency and success never seen before in human history.

Much of the technology behind this, sadly, comes from U.S. corporations that have compromised their principles; and it seems there is little the U.S. government can do about this. Put another way, the U.S., via these companies, has thus far empowered China's dictatorship on this front. PRC authorities have thus been immensely successful at censoring the online flow of news, information, and personal communication in China.

It is for this reason that the hope of Internet freedom in China rests upon the shoulders of those of us in the free world. Many like myself have realized this, and responded to the call. And this is why we now see CCP authorities using violence and thug-like tactics here on U.S. soil.

Our government first engaged China under Nixon with the aim of bringing about a "peaceful transformation" inside China; we hoped for democracy, freedom, and human rights there. Engagement was seen as the means. However, after three decades of engagement, political and religious freedom remains enormous problems in China, and freedom of the press and information continue to be abysmal. At this very moment, in fact, China's communist regime brutally suppresses tens of millions of innocent citizens, such as Christians, Tibetans, the Falun Gong, and those with differing political beliefs.

A different approach is needed today more than ever. The Internet offers just that.

OUR SOLUTION

Myself and other persons who practice Falun Gong here in America are well aware of this situation: We have ourselves been brutally persecuted by China's regime, and we are the heart of the state's censorship efforts. We have responded with all our strength and all our heart. For six years we have been proactively fighting this situation, every day. We are extremely motivated, tenacious, and uncompromising.

Our chief approach has been to give the people of China accurate, uncensored news and information about the world. Our efforts have been extensive, and include:

- launching a TV station, New Tang Dynasty Television, which is the *only* TV network that has broadcast uncensored TV programs to 40–60 million Chinese satellite dishes. We do this 24 hours a day, every day, fully unencrypted and free of charge;
- launching a newspaper, *The Epoch Times*, which is now the largest Chinese language newspaper outside of China. Over 1.5 million copies are distributed each week to Chinese communities around the world. We published *The Nine Commentaries*, which has prompted 7 million-plus Chinese to quit the Chinese Communist Party (CCP). The newspaper's website draws over 1 million hits daily from mainland China people alone;
- launching Sound of Hope Radio network, a short-wave radio broadcast that covers the entirety of China, and broadcasts hours of original programming daily.

Additionally, we have carried out a massive grassroots initiative to disseminate information in PRC China, which includes, for example:

- making 30–40 million personal phone calls into China to a) reveal censored information about state-run religious persecution, and b) encourage CCP members to resign from the Party and affiliated organizations;
- faxing on average 300,000 faxes of a similar nature to China every month;
- mailing informational documents to China, along with CDs, VCDs, and DVDs

Even greater still, though, are our Internet capabilities. This is the part of our approach that China's communist regime fears most. And this is what I wish in particular to call your attention to today. First, I would like to mention what we have accomplished so far, and then give you a sense of how much more we can accomplish in the cause of freedom. Consider the success of our companies Garden Networks for Freedom of Information Inc., UltraReach Internet, Inc., and Dynamic Internet Technology:

- In 2005, online hits by mainland Chinese users at our unblocked sites averaged some 30 million each day.
- Essentially every single website that would be blocked to mainland Chinese viewers, but that is now accessible, is accessible for one reason: we have chosen to include them among the pages we unblock.
- This is the case for the Websites of Voice of America (VOA) and Radio Free Asia (RFA)—for which we have provided this service the past four years.
- With our technology, even the uncensored search engines of Google and Yahoo are made available to Chinese users.

We are the only group that has managed to achieve this much, in the cause of freedom. No other entity worldwide—government or private sector—has even come close. And this, despite our working with limited resources. Most of our staff can only contribute part-time, due to our limited funding. Increased funding would allow us to do this work full-time. If we have accomplished all of this on a part-time, often volunteer basis: Just imagine what we could accomplish working full-time.

Secondly, I would like to share that this is only the tip of the iceberg. What I have described thus far is the success of our unblocking technology. Much greater still is the potential of the Web portal that we have built.

Our Web portal, known as WorldGate, has just been released in its second version, and contains 10 Web services as well as an enhanced search engine that finds pages which other search engines miss or block. Our search engine's capacity is currently at 200 million pages and our web services are used daily by 10,000 individuals. These figures are limited due to a lack of funding and resources. Our aspiration is to integrate our Web portal with our industry-leading anti-blocking technology so as to provide users in China with complete and transparent access to online information, community building, and publishing capability—all of which would be uncensored and unblocked. The portal will give tens of millions of people in China access to, literally, a whole new world.

Our goal is to achieve the capacity to support 20 million daily users (i.e., approximately 50% of the 120 million total projected Chinese users, assuming each user visits our portal once every 3 days on average) by the end of 2006, and to be able to support 30 million daily users (including those using wireless devices as a means of access) by the end of 2007. If this effort gains sufficient funding, the enhanced

portal could build a user base with the critical mass necessary to support itself via advertising.

What this would amount to is the closest thing Chinese citizens have ever had under CCP rule to freedom of the press, freedom of speech, and freedom of assembly. The WorldGate Web portal will empower China's people as never before. The impact would be immeasurable. At a minimum, it would allow hundreds of millions of mainland Chinese access to news and information tightly sealed off from them; they would be able to communicate and exchange ideas with one another freely; and do so, without fear of getting caught or reprisal. The positive change that would follow in Chinese society would be swift, and conducive to the stability and health of the Asian region as a whole. It would foster a dramatically better environment for U.S. businesses, bringing increased accountability, transparency, and uniformity in the application of policy and law. And it would mean that more accurate information about China would become available to those of us in the United States, something many groups would like to have.

WHAT IT TAKES

There are several reasons I am confident I and the others in my group can achieve this vision. In at least several regards we are unique.

A. Experienced Tech and Management—

Our team consists of 100+ experienced software developers, most of whom hold advanced science or engineering degrees. Our managers hold advanced technical and business degrees. For the past six years we have been developing and delivering technology to open up China's Internet and providing access to uncensored information.

B. Proven Capability—

Past and current versions of our Web technology have already garnered great success. For six years and running we have provided uncensored online news services, chat-rooms, forums, and secure email services to users inside and outside of China. We have developed a novel scheme that enables search engine crawlers to bypass China's sophisticated and well-financed Internet blockade. We have developed our own cutting-edge anti-blockade applications, designed especially for China's Internet. We have managed to unblock significant Web sites. For example, the International Broadcasting Board, which oversees VOA and RFA, has relied on us for the past four years to make its Web sites accessible. It is only through us that China's people can access the uncensored versions of Google's and Yahoo's search engines, the pages of various Western media outlets, etc. In 2005, daily hits by mainland Chinese at Web sites unblocked with our technology averaged over 30 million. We are the only group that has been able to achieve this.

C. Unshakeable Commitment—

We have a track record of establishing successful media companies, as stated above. Each has grown exponentially, becoming, in the span of a few short years, among the highest-impact Chinese language media in the world. China's communist government has used numerous methods to try to stop our media. Despite threats on our lives, physical assaults, vandalism, and many forms of intimidation, we have not for a day wavered in our efforts. We only grow more determined. We bring this same iron-clad determination to our Internet initiative. The past six years stand as testimony: We will never bow to, nor be influenced whatsoever by, China's communist regime. We will stand by our mission to the end.

D. Unmatched Know-How—

We come from China ourselves and have worked for years now on breaking China's Internet censorship. Our knowledge is unparalleled when it comes to providing access to Chinese users. Success in this battle takes more than technology: One has to know how to deploy it so that it is accessible, *and safe*, for Chinese users. This necessitates always staying one step ahead of Beijing's ever-evolving means of censoring and blocking. This we have mastered. Finally, we have the connections and know-how to publicize our product in China, and do so in a way that educates our target Chinese audience; many don't realize how much news and information is being hidden from them. We can furthermore assure them of the safety of our product; this is critical, as most Chinese users fear government monitoring and punishment.

In sum, our products are proven. Our people are dedicated. The infrastructure is in place. All that we need at this point is funding. U.S. government sponsored programs like Voice of America and Radio Free Asia are already using our software

to fulfill their mandates. With adequate funding, we can enhance our software and scale our user-base in China to rival that of the portal industry's leaders—Yahoo and Google—but do so without compromises or blocking of any sort. I would offer in closing: If you seriously wish to see a free Internet in China, we have the solution. With your support we can turn this vision into reality.

APPENDIX 1—FORBES

When All Else Fails: Threats
Richard C. Morais, 02.10.06, 5:45 PM ET

Peter Yuan Li—a key figure in the Falun Gong's technologically sophisticated attempt to undermine the Chinese Communist Party—was brutally attacked and beaten in his home in Duluth, Ga., as Forbes was going to press with its cover story on how the spiritual movement is penetrating the Chinese government's hi-tech censorship. At 11:15 A.M. on Feb. 8, according to the Fulton County Police Department Incident Report, Asian men stormed the house of the Princeton-educated information technology technician, bound and gagged and beat him, before fleeing with two 16-inch Sony laptop computers, Li's wallet and yet unknown material from his files.

"They were not looking for valuables," says Dr. Li, who needed 15 stitches in his face. "They left my daughter's jewelry and camcorder and other valuables."

Li is a Falun Gong practitioner and a technology specialist employed by the Epoch Times, a Falun Gong-affiliated newspaper that published a highly critical series of essays in a book called Nine Commentaries on the Communist Party. The Nine Commentaries was coupled with an effective promotional campaign within China that urged the CCP and related youth party members to renounce their party affiliation on specially designed Web sites (see: "Cracks In The Wall"). The Falun Gong claim 7 million Communist Party members have renounced their allegiances due to the Nine Commentaries campaign.

U.S. citizen Li says he not only maintains the Epoch Times Web site, but also the related Nine Commentaries and CCP renunciation Web sites that mainland Chinese are accessing through proxy technologies to register their displeasure with the Chinese government. Beijing has been trying to combat their efforts with the compliance of Western firms that provide the nuts and bolts of China's Internet: Cisco Systems (nasdaq: CSCO—news—people), Google (nasdaq: GOOG—news—people), Microsoft (nasdaq: MSFT—news—people), Nortel Networks (nyse: NT—news—people), Sun Microsystems (nasdaq: SUNW—news—people) and Yahoo! (nasdaq: YHOO—news—people).

The two first men who pushed their way into his home in the Atlanta suburb were armed with a knife and gun and spoke Korean, Li tells Forbes. But once they had taped his eyes and bound him, Li says he heard another one or two men enter his house. One of these men spoke to him in Mandarin and demanded to know where he kept his "locker" and documents. The intruders ransacked the house and forced open locked file cabinets. After the men left, Li was able to escape into the street, where a neighbor was able to help him and call the police.

There have been many reported incidents of Falun Gong practitioners getting harassed or threatened while on U.S. soil. Last year, for example, the San Francisco home of Houzhi Ma, an Epoch Times editor, who finances and manages reporters inside China, was repeatedly burgled. His laptops were also stolen.

Erping Zhang, spokesman for the Falun Gong, says it is no coincidence that Li's attack took place as Forbes reveals the extent of the Falun Gong's penetration of the Chinese government's information barriers. "Given that valuables were not taken; given that laptops and related Internet files and receipts were taken; and given that the attackers asked where the files were kept—it is apparent that the attackers were after Internet antiblockage and encryption information," says Zhang.

There is no evidence that the break in at Li's home is tied to the Chinese government. The Chinese embassy in Washington, D.C. did not return our call for comment.

In 2004, the U.S. Congress passed Resolution 304, which recognized "the Chinese government has attempted to silence the Falun Gong movement and Chinese prodemocracy groups inside the United States." The resolution urged the U.S. Attorney General to "investigate reports that Chinese consular officials in the U.S. have committed illegal acts while attempting to intimidate or inappropriately influence Falun Gong practitioners or local elected officials."

Dr. Haiying He, a medical oncologist at the Dana-Farber Cancer Institute at Harvard University, is also a Falun Gong activist and was one of the first CCP party members to officially and publicly renounce his membership after the Nine Commentaries campaign began. He says he has not only been threatened in person in Boston, but that his parents get regular secret police visits at their home in

Chongqing City, China. Three months ago, he says, the secret police described his "every move" in the U.S. to his parents.

Dayong Li, is a founder of the global organization that is orchestrating the CCP renouncements. He also owns a New Jersey satellite service company. Li says his parents in Hunan Province also receive similar visits, and the secret police terrorize the elderly couple by saying they know "everything" about their son—including where he walks, his salary and his company details.

"They warn me not to be active," says Li. "They tell my parents if I am, my life is in danger."

*http://www.forbes.com/technology/2006/02/10/china-falun-gong__*0210falungong.html

APPENDIX 2—BUSINESS WEEK

Outrunning China's Web Cops
Net-savvy outfits are finding ways to let citizens see banned sites
ISSUE DATE: February 20, 2006
NEWS: ANALYSIS & COMMENTARY

From an undisclosed location in North Carolina, Bill Xia is fighting a lonely war against China's censors. From morning till well into the night, the Chinese native plays a cat-and-mouse game, exploiting openings in Beijing's formidable Internet firewall and trying to keep ahead of the cybercops who patrol the Web 24–7 and have an uncanny ability to plug holes as quickly as Xia finds them. A member of the banned Chinese sect Falun Gong, Xia is so fearful that Beijing will persecute his family back in China, that he refused to be photographed for this story, reveal where exactly he was born, or even provide his age beyond saying he's in his 30s.

Xia is part of a small group of Chinese expatriates who are making a modest living helping Web surfers back home get the information their government would rather they not see. Chinese citizens hoping to read about the latest crackdown on, say, Falun Gong or the most recent peasant rebellion in the provinces can use technology provided by Xia's Dynamic Internet Technology Inc. to mask their travels to forbidden Web sites.

Voice of America (VOA) and human rights organizations also are paying DIT to help evade the censors and get their message out to the Chinese masses. Says Xiao Qiang, who teaches journalism at the University of California at Berkeley and runs the China Internet Project: "These tools have a critical impact because the people using them are journalists, writers, and opinion leaders."

So far, DIT, UltraReach, and other outfits like them have lured less than 1% of China's estimated 110 million Net users. But Google (*GOOG*) decided in January to censor information inside China, a practice already followed by Microsoft (*MSFT*) and Yahoo (*YHOO*)!, arguing that it's the only way the search engines can crack the Chinese market.

So Xia is convinced that the services he and others provide will become increasingly crucial to keep information flowing and, ultimately, he hopes, build an open society back home. "Once in a while I feel more homesick than usual," says Xia, who says he hasn't seen his family in seven years. "But it's such a great project, and it helps so many people."

The seeds of DIT were sown when Xia arrived in the U.S. for grad school in the '90s. Stunned by America's openness, he realized his perception of reality had been warped growing up in China. "I was a believer of the propaganda," he recalls. And when Xia was exposed to all of the information on the Internet, it "started tearing apart what I'd accepted before." At the same time, the repression of Falun Gong at home angered him, though he insists it is Beijing's curbs on free expression that led him to found DIT in 2001. A year later he began building up a roster of clients, including VOA, Human Rights in China (HRIC), and Radio Free Asia.

Fleeting Window

The simplicity of DIT's approach belies its effectiveness. The company distributes software, called FreeGate, which disguises the sites a person visits. In addition, DIT sends out mass e-mails to Chinese Web surfers for clients such as VOA, which is banned in China. The e-mails include a handful of temporary Web addresses that host off-limits content and springboards to other forbidden sites.

Keeping one step ahead of the censors is what this game is all about. China's cybercops are so efficient that these gateways typically stay open for only 72 hours, according to Ken Berman, an information technology director at the State Dept.-affiliated International Broadcasting Bureau, which hired DIT and UltraReach to help make VOA's Web content available in China.

Yet despite being outmanned and outspent—Xia has a tiny staff, an annual budget of about $1 million, and relies mainly on volunteers—DIT's customers say it has been remarkably successful. Xia's staff monitors the success rate of the hundreds of thousands of e-mails they send out each day. If one gets bounced back, the language must be scoured and the offending words detected and added to the company's blacklist. Workarounds are often developed, much like spammers finding holes in a corporate e-mail filter. For instance, an e-mail that contains "VOA" might get squelched, but one with a zero substituted for the "O" could get through.

As Google and other U.S. search companies increasingly cooperate with Beijing, DIT is helping the groups like HRIC break through the firewall. Before Google began censoring its results in China in January, HRIC appeared in the top three search results. Although China's Google users would have had difficulty accessing the HRIC sites, which are blocked, they at least knew they existed. Today they don't appear at all in China. But thanks to DIT and others, visitors to its Chinese-language newsletter spiked to more than 160,000 in January, up sixfold in the past 18 months. Says Xia: "If information isn't available on the Internet, it might as well not exist."

Every time something momentous happens in China—and Beijing smothers news about it—more people use his software, Xia says. In 2003, when the SARS epidemic peaked and Chinese authorities seemed to be withholding information, the number of DIT users spiked by 50%, he says—and they doubled after reports surfaced in December that Guangdong police had shot protesting villagers.

Such moments invigorate Xia, making the effort worthwhile. And by the looks of things, the services he and his peers provide will be in demand for quite a while to come.

*http://www.businessweek.com/magazine/content/06__*08/b3972061.htm

---

STATEMENT FOR THE RECORD BY MS. CHARLOTTE OLDHAM-MOORE, DIRECTOR OF GOVERNMENT RELATIONS, INTERNATIONAL CAMPAIGN FOR TIBET

The International Campaign for Tibet (ICT) is deeply concerned about U.S. technology companies assisting the Chinese government in censoring the internet and in identifying and punishing those who express views contrary to the government's. For almost twenty years, ICT has worked to promote human rights and democratic freedoms for the people of Tibet. Tibetans continue to be subject to often brutal repression at the hands of the Chinese government, and their unique religious, cultural and linguistic heritage is under assault.

An uncensored internet has enormous potential to be a liberating force and can be a vital tool for advancing human rights in Tibet. But, unfortunately, this is now not the case. Since China censors freedom of expression on the internet, and U.S. technology companies, in pursuit of new and lucrative markets, provide technology to China which is used to restrict basic freedoms; the internet is instead a tool of repression.

China's economic reforms have not led to political reforms or to fundamental improvements in its policy of controlling the flow of information. During the debates on granting China Permanent Normal Trade Relations in the 1990's, supporters argued that expanded trade with China would inexorably lead to greater human rights and democracy in China and Tibet. Regrettably, this dream has not come to pass. Instead, the Chinese government has been able to check-mate greater access to cell phones, faxes and the internet by ordinary Chinese and Tibetans by using advanced technology to censor telephone and internet communications, track cyberdissidents and disseminate propaganda. The result is a virtual Iron Curtain.

Even before Google launched its new search platform in China and Tibet, internet users there had to contend with the government's 30,000 internet police and its "great firewall," which sanitizes web search results, and blocks thousands of websites, including ICT's and other human rights organizations.

At the same time, U.S. internet companies like Microsoft, Cisco Systems, and Yahoo! have assisted China in making its repressive practices even more effective. For example, Microsoft closed a popular blog it hosted that offended Chinese censors. Cisco has sold equipment that helps Beijing restrict access to websites it considers subversive. And, in 2005 Yahoo! apparently provided information to Chinese authorities to identify Shi Tao, a Chinese journalist, who was accused of leaking "state secrets abroad." What did Shi Tao leak? Tao simply emailed portions of a directive issued by China's Propaganda Department that instructed the Chinese media as to how to cover the 15th anniversary of the military crackdown in the Tiananmen Square. And for that 'crime,' Shi Tao was sentenced last April to a ten-year prison term.

Last month, Google launched Google.cn, a new search platform in China and Tibet that censors and distorts information on topics sensitive to Beijing. Google.cn filters search results according to criteria set by the Chinese government. These topics include "Tibet," "human rights," "democracy," "Dalai Lama," and countless others. If a Tibetan or Chinese user of Google.cn, for example, wants to see an image of the 14th Dalai Lama, he will find a variety of images, but none of the exiled Dalai Lama himself. Instead, the internet user will be given images of Chinese-run Tibet, Chinese officials talking about Tibet, and even a photo of a man protesting the visit of the Dalai Lama to England. Only one of the 161 images produced by searching in Chinese for the Dalai Lama on Google.cn shows the 14th Dalai Lama, according to a February 12th report by the New York Times, and this archival photo was taken before his exile in 1959. In contrast, for people outside of China, the 2,030 unfiltered images provided on Google.com center on the14th Dalai Lama, the spiritual leader of Tibet since 1940.

While the Chinese government uses advanced technology acquired from US companies to censor internet communications and track cyber dissidents, China also uses the internet as a proactive propaganda vehicle. Chinese authorities have set up many Tibet information websites, such *www.tibetinfo.com.cn* and *www.tibetology.com.cn*, which seek to legitimatize its repressive control of the region. Never mentioning crackdowns, patriotic campaigns, and extensive human rights abuses, the English-language versions of these sites highlight living conditions in Tibet and the Chinese government's portrayal of respect for basic freedoms. These sites aim both to mould Chinese public opinion favorably towards Beijing's policies in Tibet and to mollify foreign criticism towards China's brutal record in Tibet.

For the people of Tibet, China's censorship of the internet is just one part of an overall strategy to repress their freedom of expression, and to exert control over independent information from Tibet reaching the world and "subversive" information from the outside world reaching Tibet. While the Chinese government asserts that Tibetans enjoy freedoms of speech and assembly, Tibetans in practice are not allowed, for example, to express the opinion that Tibet had ever been independent and that China's annexation of Tibet has ever been anything other than a "peaceful liberation." Tibetans continue to be arrested and imprisoned—with or without trial—and sentenced for the peaceful expression of their political views

China's continuing crackdown on the right to information in Tibet, whether via the internet or by other means, is targeted above all on those who try to publish, distribute or read the Dalai Lama's writings. A 24 year-old-monk named Phuntsok Tsering, by example, was arrested in 2001 for having a book by the Dalai Lama in his possession. He is still detained. Tashi Gyaltsen, Lobsang Dhargay, Thoe Samden, Tsultrim Phelgay and Jampel Gyatso of Drakar Trezong monastery were arrested on January 16, 2005 and are now in a labor camp in Qinghai. They are serving sentences of two to three years in labor camps for publishing a newspaper containing poems and articles of a political nature.

Although China's constitution states that its citizens have "freedom of religious belief," China aggressively censors websites and blogs on Tibetan Buddhism that do not meet the Communist Party's definition of 'acceptable' religious belief. The measures used to implement state religious policy have been particularly harsh in Tibet because of the close link between religion and Tibetan identity. Tibetan Buddhism continues to be integral element of Tibetan identity, and is therefore perceived as a threat to the authority of the state. And, the Chinese leadership views the Dalai Lama, the spiritual leader of the Tibetan people, as the main obstacle to political stability in Tibet, a "wolf in lama's clothing." As a consequence, even the display of the Dalai Lama's picture on a website or on a temple altar can result in the arrest and detention of a Tibetan. Imprisonment for terms of 5–10 years or more and brutal torture continues to be a likely consequence for monks and nuns in Tibet who express dissent.

Changing the Chinese government's policies is, of course, challenging. But, the US government can take several concrete steps to make it more difficult for China to succeed in its censorship efforts. First, the US should aggressively encourage a concerted, collective effort by American internet companies to stand up to Chinese pressure. If the companies refuse to do the right thing and take immediate action to ensure that their operations do not facilitate human rights abuses, then the pressure they are facing from the Chinese government should be matched by pressure from their own government, that of the United States.

No American company should ever, under any cirucumstances, turn over the name of a political dissident to an autocratic state with a horrific record of human rights abuses. Further, no American company whose business is the free flow of information should censor information to satisfy the political demands of a dictator-

ship. Congress must ensure that these fundamental moral lines are not crossed. And, therefore, it should pass legislation similar to the Foreign Corrupt Practices Act to bar US companies from disclosing the identities of dissidents or other individuals to foreign governments, when the information is sought to punish or control political speech, which is protected by international law. Turning over dissidents to ruthless dictatorships should clearly be prohibited by US law. American laws must support American values of freedom and advancing democracy.

Congress should also consider whether companies in violation of these fundamental principles should be banned from taxpayer financing for their foreign operations from the EximBank and OPIC, and more generally from federal procurement.

President Bush should publicly raise the crackdown on internet users in China and Tibet during his meeting with the Chinese President Hu's State Visit to the United States in April. And, Secretary Rice should make public any assistance the United States Embassy in China offered American internet companies in promoting their business in China, and whether the Embassy raised the issue of complicity in censorship with these companies.

The International Campaign for Tibet hopes that American internet companies will not put profit above principle and willfully ignore international human rights standards. But if these companies do not reverse course, Congress and the Administration must step forward to ensure that some principles are not negotiable.

RESPONSES FROM THE HONORABLE DAVID A. GROSS, DEPUTY ASSISTANT SECRETARY FOR INTERNATIONAL COMMUNICATIONS AND INFORMATION POLICY, BUREAU OF ECONOMIC AND BUSINESS AFFAIRS, U.S. DEPARTMENT OF STATE, TO QUESTIONS SUBMITTED FOR THE RECORD BY THE HONORABLE CHRISTOPHER H. SMITH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY AND VICE CHAIRMAN, COMMITTEE ON INTERNATIONAL RELATIONS, AND THE HONORABLE THOMAS G. TANCREDO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Question:

Recently, Yahoo—under criticism for turning over emails to the Chinese government that resulted in the jailing of a Chinese reporter, issued an interesting statement a few days ago. The company said, "Doing business in certain countries presents U.S. companies with challenging and complex questions . . . Private industry alone cannot effectively influence foreign government policies on issues like the free exchange of ideas, maximum access to information, and human rights reform, and we believe continued government-to-government dialogue is vital to achieve progress on these complex political issue." The reason I find this statement so interesting is because it seems to be a 180 degree turn from the kind of promises that were made to all of us in the lead up to the PNTR vote for China. Back then, private industry continually assured us that expanded commercial interaction with China would loosen Beijing's death grip on political expression. Tech and internet companies in particular assured us that the internet would be "the messenger of freedom" for China. Well, here we are just a few years later and companies like Yahoo seem to be walking away from these rosy assurances while the Chinese government has experienced a windfall of capital investment that has been effectively used to build up their military and tighten their grip on Chinese society (albeit a Chinese society with a few more cell phones, McDonalds restaurants and Wal Mart stores). Is it time for us to finally admit that economic and commercial engagement does not automatically lead to political reform, and as such, is it time for us to revisit our commercial relationship with communist China?

Response:

As President Bush has said, we want to work with China to further our mutual interests. Deputy Secretary Zoellick has remarked on several occasions that China is already integrated significantly into the international marketplace. We must work with China for it to become a responsible stakeholder in the international system, including the human rights regime. The message I and others convey to our Chinese colleagues is that allowing people the freedom to express themselves on the Internet and elsewhere does not weaken China. Instead, it promotes stability at a time of dramatic social and economic transformation. A freer China will be a healthier China, in part, because people who are free to express their views and participate in their own local governance have a stake in dealing constructively with the political, economic, and social issues confronting them. President Bush addressed the importance of Internet freedom in his recent meeting with President Hu. The Administration will continue to press China on this point.

Question:

We've heard many companies talk about how adhering to the censorship guidelines is a lesser evil than not providing service in the PRC because it will allow them to open a "crack in the door" to the world wide web for Chinese internet users. But couldn't one also make the argument that acquiescing to these demands will allow the PRC government to actually create an "alternative internet" instead, which will allow them to better control public opinion while creating the illusion of free access to information?

Response:

The PRC has committed significant resources to controlling the Internet content that is available to its citizens. It has accomplished this, in large part, by limiting the number of international gateways available and restricting access to foreign content. Its own capacity to develop and deploy censorship technologies is growing steadily. These efforts at censorship are enhanced by the preference of most Chinese Internet users for content in their own language—content that is now supplied often by PRC domestic sites. As a result, there exists already a PRC-controlled "area" of the Internet that functions incompletely but substantially as an Intranet. Nonetheless, there are Chinese Internet users who regularly employ counter-censorship measures to access forbidden content.

Question:

Many US internet companies have complained to me privately that they are being forced into accepting these kinds of "compromises" by economic pressures from Chinese competitors who enthusiastically embrace Chinese censorship requirements even while they derive tens of millions of dollars in venture capital from the U.S. market. Baidu, for example, a Chinese search engine company, recently raised enormous amounts of money in U.S. investment, only to use that funding to better control the flow of information and more rigorously restrict access to the World Wide Web by Chinese internet users. Is it time for the U.S. to re-examine the conditions under which we allow access to U.S. capital by foreign tech companies? Would the interest of expanding access to information be better served if we were to require foreign companies seeking U.S. capital to adhere to a "code of conduct" that includes vowing not to adhere to arcane censorship requirements before we allow them to access that capital?

Response:

The State Department has encouraged U.S. Internet companies, in cooperation with NGOs and other stakeholders, to develop a set of industry-wide principles with regard to their overseas activities. We understand this effort is underway, and we continue to urge our companies to make progress. The question of limiting foreign companies' access to capital in the U.S. market raises numerous policy issues, including with respect to our international trade commitments on financial services. The Department of the Treasury and the Office of the U.S. Trade Representative could address these issues in greater detail.

Questions for the Record Submitted to
Mr. Elliot Schrage by
Representative Christopher Smith and Representative Thomas Tancredo
Subcommittees on Africa, Global Human Rights, and International Operations and Asia and Pacific
For the Hearing:
"The Internet in China: A Tool for Freedom or Suppression?"
Wednesday, February 15, 2006

1. How many requests from the Chinese government or related entity on a daily or weekly average does Google, Inc. receive to censor content, provide electronic information about users, remove web logs, or update or fine tune filtering equipment?

Google's Google.cn interface began operating in February 2006. To date, Google has received fewer than a dozen requests to remove webpages from Google.cn search results. Neither the Chinese government nor any related entity has asked Google to provide electronic information about users, to remove web logs, or to update or fine-tune filtering equipment.

Google's Google.com interface continues to be freely available without censorship to all users worldwide, including in China (where the user experience may, due to filtering by Internet service providers (ISPs), be frustrating or slow).

2. Describe the legal process by which Google receives a request to censor information. What documents does the government of China present and how specific are the documents?

To date, Google has received fewer than a dozen requests to remove webpages from Google.cn search results. The several requests which have been received were communicated verbally by officials of Chinese government agencies with statutory authority to regulate Internet content, such as the Ministry for Information Industry.

Google's global Google.com interface continues to be freely available without censorship to all users worldwide, including in China.

3. Describe the established procedures for handling Chinese requests for censorship of information? Are there requests for clarification? Are there automatic referrals to U.S. headquarters/legal counsel? Are there legal appeals?

As Google has received only a handful of requests for removal of webpages on Google.cn, we are continuing to develop and refine our procedures for handling them. Google has a small group of in-house government affairs professionals in China whose responsibilities include receiving requests for removal of webpages from the relevant Chinese regulatory agencies. All requests for censorship from the government of any country in which Google operates are subject to review and evaluation by Google legal

counsel at headquarters. If any request for censorship is unclear, Google personnel would request clarification. If any request for censorship appeared to go beyond the bounds of Chinese law and regulation, Google would respond to seek appropriate limitation of the request.

Google believes that all governments should adhere to the rule of law, and follow formal legal process when issuing censorship orders and requests. Indeed, since 1999 China's Constitution has formally enshrined the concept of rule of law. However, as the Chinese government itself has periodically observed, the process of implementing a rigorous rule of law remains incomplete. Google is continuing to study and assess when it will be feasible to require censorship orders to be transmitted in formal, written form. It is our hope that such requirements will be part of any standards and guidelines adopted through the ongoing inter-industry dialogue.

We emphasize, again, that Google's Google.com interface continues to be freely available without censorship to all users worldwide, including in China (where the user experience may, due to filtering by ISPs, be frustrating or slow).

4. Under what circumstances would Google refuse a Chinese request?

Google would refuse a request for censorship on Google.cn which does not appear to be authorized under published Chinese laws and regulations.

5. Please provide the list of words and web sites the government of China has given to Google to censor or block access to electronic information.

The government of China has not given to Google any list of words and websites to censor or block.

6. Is Google required by the government of China to censor information related to China's one-child policy?

No.

7. Is Google depositing a long-term cookie on Chinese users' computers, if the computer is configured to accept cookies? When do Google cookies expire?

Google uses both session cookies and persistent cookies. These are standard and conventional practices utilized by most commercial websites worldwide. Cookies themselves do not include any private, personal, or confidential information. Rather, they make websites easier to use by allowing users to save settings and preferences from one session to another. Users have the option of deleting Google cookies at any time. Users may also disallow cookies and still continue to utilize some Google services, like the Google search engine.

Session cookies expire at the end of a session. The expiration date for permanent cookies is nearly always set at January 17, 2038. This is true not only for Google, but for nearly all websites that use permanent cookies. Permanent cookies can be deleted by users at any time.

8. Is Google logging user IP addresses? Are user IP addresses matched to the Google cookie, or can they be?
9. Are users' search terms logged by IP address?
10. Are users' search terms logged by cookie ID?
11. Can users' search terms be tied to either a cookie or an IP address?
12. How long is Google storing logged IP addresses?

First, it is important to note that Google will not operate services in restrictive jurisdictions in ways that would jeopardize the privacy and confidentiality of our users' information. For example, Google does not offer its Gmail or Blogger services via the Google.cn website. Moreover, users who have particular concerns over the privacy of their web searches, or the confidentiality of their information, can always access Google services through the Google.com website, to the extent their ISPs make it available to them.

More generally, when a user visits Google, we send one or more "cookies" to the user's computer. A cookie is a small file containing a string of characters that is sent to the user's computer when she/he visits a website. When the user visits the website again, the cookie allows that site to recognize the browser. Cookies are used to associate stored user preferences with the browser. Google uses cookies to improve the quality of our service by storing unique preferences and tracking user trends, such as how people search. The browser may be set to accept cookies, but users can also set browsers to refuse all cookies or to indicate when a cookie is being sent.

As with most websites, Google servers automatically record the page requests made when users visit our sites. These "server logs" typically include the web request, IP address, browser type, browser language, the date and time of the request and one or more cookies that may uniquely identify the browser. Google does not have a standard fixed period for storage of all server logs.

13. Many U.S. companies -- Google comes to mind -- have been quick to point out that they reached a "compromise" with Chinese authorities for providing search engine technology to Chinese users under the premise that "getting their nose under the tent" will help them to expand access to information in the future. What happens, however, if the Chinese government tries to exert more control over your companies in the future -- conceivably after your companies are more heavily invested in China's economy? Will your companies adhere to these new restrictions in the interest of shareholder profits -- or is there an ideological line in the sand that you will not cross for money?

Google's entry into the Chinese market is based upon our ability to adhere to a set of crucial lines that we have drawn. For example, we provide disclosure to our Chinese users when results have been removed from the Google.cn search index; we provide an uncensored Chinese-language interface on Google.com; and we will operate our services in ways that do not place the privacy and confidentiality of our users' information at risk. If the bases on which Google entered the Chinese market change in fundamental ways, we will not hesitate to reconsider our decision to operate there.

14. Many of my constituents have asked me what many companies in your industry are adhering to a "double standard" when it comes to cooperation with world governments. Google, for example, has resisted efforts by the U.S. Justice Department to obtain certain information associated with user searches for pornographic material on the internet -- this at the same time that the company was actively searching for a way to accommodate demands for content control from the PRC government as a condition of providing service to Chinese internet users. Why is it that it's ok to fight the demands of the U.S. government on principle when it comes to government compliance, yet it is perfectly acceptable to comply with the demands of the Chinese government? Is the libertarian ethic of internet companies selective based on revenue projections?

Google's actions in these two cases are entirely consistent: In both cases, we have acted to protect the privacy and confidentiality of our users' data. We adhere to a globally consistent policy of acting to protect our users' expectations of privacy and confidentiality.

In the case of the Department of Justice subpoena, we determined that the Department's request for billions of search queries and URLs was overbroad, overly burdensome, and irrelevant to the underlying litigation. And we used the available legal avenues to challenge the subpoena. The federal court largely agreed with our determination, quashing the Department's request for users' search queries, and sharply reducing the scope of the request for a random sample of URLs from Google's search index.

In the case of China, Google has decided not to operate on servers in China those services that would require the storage or disclosure of personally identifiable information.

Questions for the Record Submitted to
Mr. Mark Chandler by
Representatives Christopher Smith, Representative Thomas Tancredo
Subcommittees on Africa, Global Human Rights, and International Operations and Asia and Pacific
For the Hearing:
"The Internet in China: A Tool for Freedom or Suppression?"
Wednesday, February 15, 2006

Given the broad nature of the questions posed to Cisco, the following responses are intended to provide information on the scope of Cisco's activities in China and worldwide. Some of the information sought is business-proprietary and cannot be placed in the public domain given Cisco's substantial worldwide competitive and network security requirements. We will be happy to work with the Subcommittee as appropriate to provide any required access to information that for these reasons is not included in this response.

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

1. **What training has Cisco Systems, Inc. conducted in China? List specific companies and individuals, along with corporate or government affiliation.**

Cisco provides some degree of training, including directly by means of seminars and customer support, both on-line and telephonic, or indirectly by means of technical and training manuals provided to third party training institutions to almost all of our customers – which include service providers, enterprises (or large businesses), government and public sector customers and small and medium size enterprises. There are literally thousands of such customers in China, and therefore no comprehensive catalog of all such training exists or is feasible to create. Below is a discussion of the types of training provided, and the manner in which materials used for training can be accessed. To the best of our knowledge, no specialized training was provided in China that would differ in substance from that provided throughout the world.

A comprehensive set of training resources, from instructor-led courses to remote access labs and e-learning solutions, are available through authorized Cisco Learning Partners for improving technology expertise. Cisco Learning Partners are the only source of authorized Cisco training. Our general training is provided directly to our customers to optimize use of our products, or indirectly through training we provide to our independent network integrators and channel partners who design, sell and service the vast majority of networks using Cisco equipment worldwide. The principal modality for training the independent integrators and channel partners is through the development of a

curriculum and subsequent testing in order to certify them through our Cisco Career Certifications. A listing of Cisco distributors and reseller partners is listed below in an Addendum.

There are three levels of Cisco Career Certification: Associate, Professional, and Expert (CCIE; representing the highest level of achievement). There are six different paths: Various paths (or tracks) such as Routing and Switching, Network Security, and Service Provider are available so that individuals can match their certification path to their job or industry. In addition to general certifications, network professionals can enhance their core networking knowledge by achieving specialist certification in technologies such as security, IP telephony, and wireless. For more information on Cisco certifications worldwide, please see:
http://www.cisco.com/web/learning/le3/learning_career_certifications_and_learning_paths_home.html

For training on Cisco equipment, please see:
http://www.cisco.com/web/learning/le31/learning_learning_resources_home.html

If the Subcommittee would like more information on Cisco certifications or training, we would be happy to accommodate.

Cisco Networking Academy Program
In addition, we provide curriculum to over 10,000 high schools, technical schools, colleges, universities and community-based organizations worldwide, including in China, which qualify as "Cisco Networking Academies"; we do not, however, provide the teachers or the direct training conducted in those facilities.

Since its inception, over 1.6 million students have enrolled at these academies, which are located in high schools, technical schools, colleges, universities, and community-based organizations. Of the 10,000 Cisco Networking Academies, 206 are in China which have, to date, trained 28,729 students in general networking technology. There are currently 13,958 students in Networking Academy Programs in China. (Copied below is a listing and locations of the Cisco Networking Academies in China – Addendum #2.)
For more information on Cisco Networking Academies, please see:
http://www.cisco.com/web/learning/netacad/

Cisco has been a long-time proponent of blending technology and education. The Cisco Networking Academy Program is a comprehensive e-learning program that provides students with the Internet technology skills essential in a global economy. The Networking Academy delivers web-based content, online assessment, student performance tracking, hands-on labs, instructor training and support, and preparation for industry standard certifications. The Networking Academies are not run by Cisco, but we do provide the online curriculum and online testing. The classes are hands-on, leader-led and Cisco provides equipment for training purposes to Networking Academies at a discount. Due to the proprietary nature of these materials and the competitive value they hold worldwide, we only provide this to registered Cisco Networking Academy

participants. However, if the Subcommittee is interested in accessing this information, we will work with Staff to facilitate such access.

2. **Please provide copies of the exact training manuals used in China. (in English or Chinese.)**

Due to the global nature of our business and the standard technologies we provide to our customers, Cisco provides standard training manuals for our products in multiple languages. Thus, the manuals that are used by customers in the US are the same as those in China. For a complete library of these manuals, please access the following URL:
http://www.ciscopress.com/bookstore/index.asp
Or: http://www.cisco.com/web/about/ac123/ac220/about_cisco_cisco_press.html

We have provided the Subcommittee a hard copy of a popular training handbook – *Internetworking Technologies Handbook*, Fourth Edition, An Essential Reference For Every Network Professional, Cisco Press, 2004.
http://www.ciscopress.com/title/1587051192

In the Chinese language, training and testing handbooks are available at:
http://rights.pearsoned.com/
Please go to "Product Search" and type "Cisco" in the title field.

We would be pleased to provide the Subcommittee a hard-copy version of any training manuals listed on these sites.

3. **Please provide copies of the briefing books used to train Cisco employees who are training or teaching others on the use of Cisco equipment.**

There are technical educational manuals on all facets of networking technology which can be accessed at: http://www.ciscopress.com/bookstore/index.asp or through:
http://www.cisco.com/web/about/ac123/ac220/about_cisco_cisco_press.html

As noted in response to question #1, there are Cisco Networking Academies worldwide and in China. The student and teacher "manuals" for the Cisco Networking Academies are all provided online. Due to the proprietary nature of these materials and the competitive value they hold worldwide, we only provide this to registered Cisco Networking Academy participants. However, if the Subcommittee is interested in accessing this information, we will work with Staff to facilitate such access.

4. **Are American Cisco employees training Chinese government personnel on the use of Cisco equipment?**

To the best of our knowledge, no American Cisco employees are delegated or deployed to train Chinese government personnel on the use of Cisco equipment.

Like many multinational IT companies, we do have customer call centers worldwide that are available 24x7, which are periodically staffed by American Cisco employees The Cisco call centers provide routine assistance in response to specific customer questions or problems, which could constitute training, or help. Government customers in China, as all customers worldwide, may make use of this technical support.

5. **Please provide copies of workbooks and/or technical manuals given to Chinese customers for training and/or for technical support.**

Please, see #2 and #3.

6. **Please provide technical specifications for all materials sold to the Chinese government and private entities.**

The Cisco products that were purchased in China in Cisco's FY2005 are listed below. All of the technical specifications and documentation are available here: http://www.cisco.com/public/support/tac/documentation.html

Routing:
http://www.cisco.com/en/US/products/hw/routers/tsd_products_support_category_home.html

1. Cisco 12000 Series
2. Cisco uBR10012 Universal Broadband Router
3. Cisco 10000 Series
4. Cisco uBR900 Series Cable Access Router
5. Cisco 7600 Series
6. Cisco 7500 Series
7. Cisco 7400 Series
8. Cisco 7300 Series
9. Cisco uBR7200 Series Broadband Router
10. Cisco 7200 Series
11. Cisco uBR7100 Series Broadband Router
12. Cisco SN 5400 Series Storage Router
13. Cisco 3800 Series
14. Cisco 3700 Series
15. Cisco 3600 Series
16. Cisco 2600 Series
17. Cisco 2800 Series
18. Cisco MWR 1900 Mobile Wireless Router
19. Cisco 1800 Series

20. Cisco 1700 Series
21. Cisco 1600 Series
22. Cisco 800 Series

Switches:
http://www.cisco.com/en/US/products/hw/switches/tsd_products_support_category_home.html

1. Cisco MDS 9500 Series
2. Cisco MGX 8800 Series
3. Cisco BPX 8600 Software
4. Cisco Catalyst 8500 Series
5. Cisco IGX 8400 Series
6. Cisco Catalyst 6500 Series
7. Cisco Catalyst 6000 Series
8. Cisco Catalyst 5000 Series
9. Cisco Catalyst 4500 Series
10. Cisco Catalyst 4000 Series
11. Cisco Catalyst 3750 Series
12. Cisco Catalyst 3560 Series
13. Cisco Catalyst 3550 Series
14. Cisco Catalyst 3500 XL Series
15. Cisco Catalyst 3000 Series
16. Cisco Catalyst 2970 Series
17. Cisco Catalyst 2950 Series
18. Cisco Catalyst 2940 Series
19. Cisco Catalyst 2900 Series

Wireless:
http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

1. Cisco Aironet 1400 Series
2. Cisco Aironet 1300 Series
3. Cisco Aironet 1200 Series
4. Cisco Aironet 1100 Series
5. Cisco Aironet 350 Series
6. Cisco Content Services Gateway
7. Cisco Packet Data Serving Node
8. Cisco GPRS Gateway Support Node Service Manager

Voice and IP Communications:
http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

1. Cisco Phone

2. Cisco Call Manager
3. Cisco Unity
4. Cisco ATA 180 Series Analog Telephone Adaptors
5. Cisco Unified Videoconferencing 3500 Series Videoconferencing Products
6. Cisco VPN 3002 Hardware Clients
7. Cisco IAD 2400 Series Integrated Access Devices
8. Cisco MeetingPlace
9. Cisco PGW 2200 Softswitch

Optical Networking:
http://www.cisco.com/en/US/products/hw/optical/tsd_products_support_category_home.html

1. Cisco ONS 15550 Series
2. Cisco ONS 15500 Series
3. Cisco ONS 15400 Series
4. Cisco ONS 15300 Series
5. Cisco Transport Manager

Network Security Support Services:
http://www.cisco.com/en/US/products/hw/vpndevc/tsd_products_support_category_home.html

1. Cisco ASA 5500 Series Adaptive Security Appliance
2. Cisco PIX 500 Series Security Appliance
3. Cisco Secure Access Control Server
4. Intrusion Detection System (IDS)
5. Cisco Security Monitoring, Analysis and Response System
6. Cisco Secure User Registration Tool

Network Management:
http://www.cisco.com/en/US/products/sw/netmgtsw/tsd_products_support_category_home.html

1. LAN Management Solution
2. CiscoWorks Small Network Management Solution
3. CiscoWorks Security Information Management Solution
4. CiscoWorks Wireless LAN Solution Engine
5. CiscoWorks IP Telephony Environment Monitor
6. CiscoWorks QoS Policy Manager

Long Range Ethernet:
http://www.cisco.com/en/US/products/hw/modems/tsd_products_support_category_home.html

7. Please provide technical specifications for data architectures set up for Chinese customers.

Data architectures set up for customers are proprietary throughout the world, for competitive and network security reasons.

There are data architectures that are indicative of customer delivered solutions and they are readily available on our website. (Note: Adobe Reader can be downloaded here: http://www.adobe.com/products/acrobat/readstep2.html)

Please view:
Cisco Data Center Architecture:

- http://www.cisco.com/application/pdf/en/us/guest/netsol/ns377/c643/cdccont_0900aecd802c9a4f.pdf
- http://www.cisco.com/application/pdf/en/us/guest/netsol/ns224/c643/cdccont_0900aecd80404988.pdf

Networking Solutions for Large Enterprise:

- http://www.cisco.com/en/US/netsol/ns340/ns394/networking_solutions_market_segment_solutions_home.html

Cisco Vision for Service Providers:

- http://www.cisco.com/application/pdf/en/us/guest/netsol/ns537/c654/cdccont_0900aecd8039ae26.pdf

Cisco Metropolitan Mobile Network Solutions:

- http://www.cisco.com/application/pdf/en/us/guest/products/ps272/c1031/cdccont_0900aecd800fe95e.pdf

Further, as stated in our testimony, and applicable to this answer, Cisco is not a service provider or manager of networks; any data architecture that is set up can be altered at any time without our knowledge.

Addendum to Question #1 – List of Cisco Distributors and Resellers in China

Cisco Channel Partner Program: The Cisco Channel Partner Program trains and enables our channel partners to find new business, grow integrated advanced technology, and adapt to sell solutions.

Cisco Registered Partner: Being a Registered Partner is a requirement of becoming a Cisco Certified Partner and/or Cisco Specialized Partner.

Cisco Specialized Partner: The Cisco Specialized Partner program allows an organization to develop its expertise in technologies, solutions, and services. Specialization is required in order to qualify for the Certified Partner program.

Cisco Certified Partner: The Cisco Certified Partner program integrates the technology

focus of Cisco channel specializations, flexible individual career certification requirements, customer satisfaction tools, and pre- and post-sales support capabilities.

Three levels of certification are offered:

- Gold offers the highest credibility in the marketplace. Cisco Gold Certified Partners deliver the highest level of support, have achieved a measurable level of customer satisfaction, and are typically recognized for gaining expertise in three specializations.
- Silver offers a company enhanced credibility, provides objective evidence of superior service and support capabilities, and recognizes a focus on at least two specializations.
- Premier offers a company credibility and access to Cisco programs, as well as recognition for focusing on at least one specialization.

More information on the reseller program can be found at:
http://www.cisco.com/web/partners/pr11/index.html

Cisco Channel Partner Program Requirements:
http://www.cisco.com/warp/public/765/partner_programs/channel_partner_program_requirements.shtml

We have three general distributors in China, who are authorized to supply products to end users and to resell to other resellers: Digital China, Ingram Micro and Xiao Tong.

Below is a list of our channel partners in China who are authorized to resell products in conjunction with system integration services which they supply to end users, based on their own capabilities.
(You may also find this info on this website:
http://www.cisco.com/global/CN/partners/partner_finder/partner_finder_cooperate.shtml)

金牌认证合作伙伴(Gold)

查询金牌认证合作伙伴BEID

金牌认证合作伙伴	
万达信息股份有限公司	SHANGHAI WONDERS INFORMATION CO.，LTD.
上海华讯网络系统有限公司	ECCOM Network System Ltd.
上海金陵时威科技发展股份有限公司	Shanghai Shiwei Network System Engineering Co.， Ltd.

智汇科技（中国）有限公司	COMMVERGE SOLUTIONS (ASIA) CO LTD
科联集成有限公司	Computer And Technologies Integration Limited
东软软件股份有限公司	Shenyang Neu-Alpine Software Co.， Ltd.
中国惠普有限公司	China Hewlett-Packard Co.， Ltd. (Beijing Head Office)
中盈优创资讯科技有限公司	Unihub China Information
中联电脑(国际)有限公司	VANDA COMPUTER & EQUIPMENT CO.， LTD.
中铁信息工程集团有限公司	SinoRail information engineering Group
云南南天电子信息产业股份有限公司	YUNNAN NANTIAN ELECTRONIC INFORMATION CO.， LTD
亚信科技（中国）有限公司	AsiaInfo Technologies (China)， Inc.
亿阳信通股份有限公司	Bright Oceans Inter-Telecom Corporation
北京先进数通信息技术有限公司	ADVANCED DIGITAL TECHNOLOGY COMPANY LTD
北京合力金桥系统集成技术有限公司	Beijing Hollybridge Co，.Ltd
北京同天科技有限公司	Town Sky International Limited
北京四达时代通讯网络技术有限公司	Beijing Star Communication Network Technology Co.， Ltd.
北京天桥北大青鸟科技股份有限公司	Tian Qiao Beida Jade Bird Sci-Te Co
北京宏天德美数码科技有限公司	Beijing DMX Technologies Limited
北京宝亮网智电子信息技术有限公司	Beijing Polybright Intellnet Electronic Information Technology Co.，Ltd.
北京市太极华青信息系统有限公司	Beijing TaijiHuaqing Info.System Co.，Ltd
北京康达联科信息技术有限公司	BEIJING COM-LINK INFORMATION & TECHNOLOGY CO
北京新晨科技股份有限公司	Beijing Brilliance Technology Co.，Ltd.
北京新脉远望科技有限公司	Beijing Cyberplus Technology Co.， Ltd
北京神州新桥科技有限公司	BEIJING SINO-BRIDGE TECHNOLOGY LTD
北京能通万维网络科技有限公司	BEIJING NTONG NETWORKS TECHNOLOGY CO LTD

北鹰科技有限公司	North Eagle Technology Co.， Ltd
国际商业机器中国有限公司	IBM China Company Limited
威发系统（中国）有限公司	WAFER SYSTEMS (China) Ltd.
宇广网络系统有限公司	EQUANT INTEGRATION SERVICES
方正奥德计算机系统有限公司	Founder Order Computer System Co.， Ltd.
电讯盈科（北京）有限公司	PCCW BEIJING LTD
神州数码集成系统有限公司	Digital China Holdings Limited
达科数据通讯中国/香港有限公司	Datacraft China/Hong Kong Limited
高威电信（广州）有限公司	Macroview Holding Co. Ltd
南京南大金利得电子科技有限公司	Gold Leader Electronic Science & Tech. Co.， Ltd.
南京联创科技股份有限公司	LINKAGE SYSTEM INTERGRATION CO.， LTD.
江苏金智科技股份有限公司	Wiscom System co.，Ltd
广东天图科技有限公司	Guangdong Grand Cycle TechnologyCo.， Ltd.
广州新华时代数据系统有限公司	Times Data System Co.，Ltd.
特灵达新时技术有限公司	Telindus Technology Co.， Ltd.
杭州荣志网络系统工程有限公司	HANGZHOU LONGZHI NETWORK SYSTEM
浙江大学快威科技集团有限公司	Zhejiang University Qware Technology Group Co.， Ltd.
深圳市紫金支点技术股份有限公司	SHENZHEN ZIJIN FULCRUM TECHNOLOGY CO.， LTD.
英思达计算机系统(深圳)有限公司	Shenzhen INFO-STAR Computer Systems Co.，Ltd.
黎明网络有限公司	Liming Networks Systems Co.，Ltd
金科集团(香港)有限公司	Goldtech Group Co.

返回顶部

银牌认证合作伙伴 (Silver)

查询银牌认证合作伙伴BEID

银牌认证合作伙伴

三力网络有限公司	3DTGNT NETWORKS CO.，LTD.
上海亚太蓝星计算机信息技术有限公司	Shanghai Aisa&Pacific Lan Star Network Engineering Co.， Ltd.
上海宝信软件股份有限公司	SHANGHAI BAOSIGHT SOFTWARE CO.， LTD
上海广电通讯网络有限公司	SHANGHAI SVA COMMUNICATION CO LTD
上海时光科技发展有限公司	Time Technology Development Co.，LTD
上海玺辰信息系统有限公司	CGEN Information System Co.，Ltd.
上海网赢信息系统有限公司	NetStar Group (China)
上海致达信息产业股份有限公司	Shanghai Zenitek Information Industry Co.，Ltd
上海邮电电脑有限公司	SHANGHAI P&T COMPUTER SYSTEM CO.，LTD.
上海银欣高新技术发展股份有限公司	SHANGHAI YINXIN NEW TECHNOLOGY DEVELOPMENT CO.，LTD
深圳市颖众电脑有限公司上海分公司	STEPTECH INC. (CHINA)
中太数据通信有限公司	Zoom Networks Inc.
北京中青旅海天数码科技有限公司	Beijing Cytsesky Digital Technology Co.Ltd.
北京华夏电通科技有限公司	BEIJING POWERCOM TECHNOLOGIES LTD
北京威亚斯科技有限公司	Beijing viyas Co.， Ltd
北京威奥特信通科技有限公司	BEIJING WAYOUT TELECOM TECHNOLOGY CO.，LTD.
北京宇信鸿泰科技发展有限公司	Beijing SI Hitech Co.，Ltd.

北京惠天九州科技有限公司	Beijing Huitian Xuye Technology Co. , Ltd.
北京新宇系统集成有限公司	Xiamen Newsky Software Co. , Ltd
北京易诚智讯科技发展有限责任公司	Beijing INTELLICOM Technology Co. , Ltd
北京网鼎系统集成有限责任公司	Winning Network System Integration Co. , Ltd.
北京联信永益科技有限公司	SUREKAM CORPORATION
北京艾提科信网络技术有限公司	BEIJING IT RESOURCES TELECOM TECHNOLOGY
北京西门子通信网络股份有限公司	Siemens Communication Networks Ltd. , Beijing
北京赛文世纪信息系统有限公司	BEIJING SEVENET INFORMATION TECHNOLOGY COMP
北京龙翔达信息技术有限公司	BEIJING LXD INFORMATION TECHONOGIES LTD.
太极计算机股份有限公司	TAIJI COMPUTER CORP.
西安海星计算机系统集成技术有限责任公司	Xi'an Seastar Computer System Integration Tech.Co. , Ltd.
华南资讯科技有限公司	SINOBEST INFORMATION TECHNOLOGY LTD
广东中实通信技术有限公司	GUANGDONG TRUSTOL COMMUNICATION TECHNOLOGY CO
广州市金税信息系统集成有限公司	GUANGZHOU KINTH COMPUTER CO LTD
联想中望系统服务有限公司	China Weal Business Machinery Co. , Ltd.
现代设备(中国)有限公司	MODERN DEVICES LTD
杭州怡德数码技术有限公司	HANGZHOU DELTEQ DIGITAL TECHNOLOGY CO LTD
浙江鸿程计算机系统有限公司	ZHEJIANG HONGCHENG COMPUTER SYSTEM CO. , LTD
浪潮集团有限公司	LANGCHAO GROUP LTD.
深圳市凌格科技有限公司	SHENZHEN LINK COMMUNICATION SYSTEM

	EQUIPMENT CO.，LTD.
深圳市和讯科技有限公司	Shenzhen Hicent Technology Ltd.
深圳市新太科技有限公司	Shenzhen Suntek Technology Co.，Ltd
深圳市方迪计算机系统有限公司	Shenzhen fortune computer system co.，ltd
重庆菲斯特信息网络有限责任公司	Chongqing First Information & Network Co.，Ltd.

高级认证代理商 (Premier Reseller)

查询高级认证代理商北京区BEID

北京

北京航天新概念软件有限公司	AEROSPACE NEW CONCEPT SOFTWARE CO.，LTD	北京
北京赛尔思科技有限公司	Beijing Wealth Tech CO.，LTD	北京
北京溢德通达科技有限公司	Beijing Bui-Net Systems.Co.Ltd.	北京
北京宽太视通软件技术有限公司	Beijing KT Network Technology Co.，Ltd.	北京
北京凯文斯科技发展有限公司	Beijing KVS Science&Tech Development Co.，Ltd	北京
北京雷恒科技有限公司	beijing leiheng science & technology co.，ltd	北京
北京隆鑫泰业科技有限公司	beijing longxintaiye technology co.，ltd	北京
北京欣邦宝通计算机网络系统有限公司	BEIJING MERRY BOND NETWORK SYSTEMS LTD	北京
北京网联盈通科技有限公司	Beijing NetLink Science&Technology Co.，Ltd	北京
北京捷先科技有限公司	Beijing Newbase Science&Technology Co.， Ltd.	北京
北京缘发生茂网络技术有限公司	Beijing Run-fast Network Technology Co.，Ltd	北京

北京天扬昊海科技发展有限公司	Beijing S.M.O Technology Development Co.，ltd	北京
北京世纪恒安科技发展有限公司	Beijing Shiji Hengan Technology Development CO.，LTD	北京
北京双鑫汇在线科技有限公司	Beijing Shuangxinhui Technology Co.，Ltd	北京
北京神州黎明网络技术有限公司	Beijing Sinodawning Network Technology Co.，Ltd	北京
北京三川智远科技有限公司	Beijing Sun-train Technology CO.，LTD.	北京
北京迪安伟业科贸有限责任公司	BEIJING TECH. CO.， LTD.	北京
北京中联科通电子系统工程科技有限公司	Beijing techview system engineering inc.，Ltd	北京
北京天创仁合科技发展有限公司	Beijing TianChuangRenHe Technology Development Co .，Ltd	北京
北京天佑永续网络技术有限公司	BEIJING TIANYOUYONGXU NETWORKS CO LTD	北京
北京同方嘉地科技有限责任公司	BEIJING TONGFANG KARDY TECHNOLOGY CO.LTD	北京
北京通天至达科技发展有限公司	Beijing Tongtian Zhida Science&Technology Development CO.，Ltd	北京
北京天融信网络安全技术有限公司	Beijing Topsec Science and Technology Co.， Ltd.	北京
北京太行兴业科技有限公司	beijing totop technolgy co.，ltd	北京
北京泰信邦计算机系统网络工程技术有限公司	BEIJING TSB COMPUTER SYSTEM & NETWORK ENGINEERING CO.LTD	北京
北京网联信通科技有限公司	Beijing WangLianXinTong Technology CL.，Ltd	北京
北京网锐通达科技有限公司	Beijing Wangrui Tongda Technology Co.， Ltd	北京
北京阳光世远科技发展有限公司	Beijing Yangguna Shiyuan Technology Development Co.，Ltd	北京

北京亿海恒达科技有限公司	Beijing YHHD technology	北京
北京亿海兰特科技发展有限公司	BEIJING YI HAI LAN TE CO.LTD	北京
北京怡华通联信息技术有限公司	BEIJING YIHUA TONGLIAN INFORMATION TECH.CO.，LTD.	北京
北京震天网络科技有限公司	BEIJING ZHENTIAN NETWORK TECH CO LTD	北京
北京智达鑫业经贸有限责任公司	BEIJING ZHI DA XIN YE TRADE CO.，LTD.	北京
北京中育远恒科技有限公司	Beijing zhongyuyuanheng technology co.，ltd	北京
北京赛科世杰科技发展有限责任公司	BeijingSuperherosHigh Technology Development co.，Ltd	北京
中国软件与技术服务股份有限公司	CS&S NETWORK TECHNOLOGY CO. LTD.	北京
卓优数据科技有限公司	Joyou Data Technology Ltd，Co.	北京
北京凯英信业科技有限责任公司	Keytec Computer&Information System Co.，Ltd	北京
日电信息系统（中国）有限公司	NEC SYSTEMS INTEGRATION(CHINA)CO.，LTD	北京
北京九瑞网络科技有限责任公司	Nine Max International Inc.	北京
伟令达信息技术有限公司	SHENZHEN WELLPLUS NETWORKS CO LTD	北京
北京思奥特科技发展有限公司	THROUGHOUT LTD	北京
北京市天正利达科技发展有限公司	tianshenglida	北京
京汇企业(香港)有限公司	KINGSWELL ENTERPRISES (H.K.)LTD.	北京
赞华(北京)电子系统有限公司	NIKOYO (BEIJING) ELECTRONICS SYSTEMS CO.，LTD.	北京
北京华诚动力科技发展有限公司	Bei Jing Hua Cheng Power Technologies Co.，Ltd	北京
北京佳华通达科技发展有限公司	Beijin Jiahuatongda Technologies Development Co.，Ltd	北京

北京爱创世纪科技有限公司	Beijing Acctrue Century Tech.Co.，Ltd	北京
北京时代飞扬科技有限公司	Beijing Age-Fly Technology Co.，Ltd	北京
北京亚联美讯科技发展有限公司	BEIJING ASIA LINK TECHNOLOGY CO LTD	北京
北京北方博业科技发展有限公司	Beijing beifangboye technology development co.，ltd	北京
北京浩辉京鼎科技有限公司	BEIJING BEIKE TECHNOLOGY CO LTD	北京
北京世纪盈联电子技术有限公司	Beijing Century Elink Electronic Technology Co.， Ltd.	北京
北京黎明纪元科技发展有限公司	Beijing Centurydawn Technology&Development Co.，Ltd	北京
北京创亿新联数码技术有限公司	beijing choice digital technology co.，ltd	北京
北京康普力特信息技术有限责任公司	BEIJING COMPUT INFORMATION TECHNOLOGY CO.，LTD	北京
北京中油科锐星科技发展有限公司	Beijing Creattion CO.，LTD	北京
北京易电科创科技有限公司	Beijing Editeq Technology Co，Ltd.	北京
北京友创佳业科技有限责任公司	Beijing Friendly Creative technology Co.，ltd	北京
北京佳易恒瑞科技有限公司	Beijing Good Easy server CO.，Ltd	北京
北京国都时代科技有限公司	beijing guodutimes science & technology co.，ltd	北京
北京翰明恒业数码科技有限公司	Beijing Hanminghengye Digital Technology Co	北京
北京恒远至达科技发展有限公司	Beijing Hengyuanzhida Science&Technology Development Co.，Ltd	北京
北京华创力合科技发展有限公司	Beijing Huachuang Lihe Science and Technology Develpoment Co.Ltd	北京
北京华陆信达网络科技有限公司	Beijing Hualuxinda network&Technology Co.Ltd	北京

北京翌丰恒达网络系统工程有限公司	BEIJING INFINITE NETWORK SYSTEM CO LTD	北京
北京嘉和正太科技有限公司	Beijing Jiahezhengtai Science & tech Co.，Ltd	北京
北京佳兴拓展科技有限公司	Beijing JiaXingTuoZhan Technology Co.，Ltd FaxRegion	北京
北京杰迅鸿翔信息技术有限公司	Beijing Jiexun Hongxiang Information Technology Co.， Ltd.	北京
北京金捷龙科技有限公司	Beijing JinJieLong Science Technology Co.，Ltd	北京
北京奇迹科汇科技有限公司	Beijing Miracle Valley Technology Co.，Ltd	北京
北京北科时代科技有限公司	Beijing NorthTek Technology Co.，Ltd.	北京
北京西伯尔通信科技有限公司	Beijing XBELL Communication Technology Co.，Ltd	北京
北京中科视讯科技有限公司	Beijing? zhongkeshixun tch .cn	北京
北京合力网兴科技发展有限公司	BEIJING?? HLWX Technology Co.， Ltd.	北京
北京比蒙正太计算机技术有限公司	Bimeng Zhengtai Computer Technology Co.，Ltd.	北京
北京中软融鑫计算机系统工程有限公司	CHINA RESOFT COMPUTER SYSTEM ENGINEERING CO	北京
北京市东正利华科技有限责任公司	Dong Zheng Li Hua Technology CO.，LTD	北京
长城计算机软件与系统有限公司	Great Wall computer software &systems INC	北京
鸿丰迅通网络技术（北京）有限公司	HFCOM Network Technology	北京
北京恒创开源科技发展有限公司	HIGH FOREVER(China)Co.，Ltd	北京
海联讯信息网络科技（深圳）有限公司	Hirisun Infonet Technology(Shenzhen)Co.， Limited	北京
北京华纬讯电信技术有限公司	sinowave communications Ltd.	北京
北京希创技术有限公司	Systron Technologies Co.， Ltd.	北京

北京蔚蓝世纪科技有限公司	BEIJING BLUE MILLENIUM SCIENCE AND TECHNOLOGY	北京
北京中网基业数码技术有限公司	BEIJING CHIEF DOM DIGTAL TECHNOLOGY CO LTD	北京
北京东华合创数码科技股份有限公司	BEIJING DONGHUA COMPUTER & SYSTEM CORP.	北京
北京阳光金网科技发展有限公司	BEIJING GOLD SUNSHINE NET TECHNOLOGY DEVELOPMENT CO. LTD.	北京
AT&T (中国)有限公司	ATT CORP	北京
北京华胜天成科技股份有限公司	Beijing Teamsun Technology Co.， Ltd.	北京

查询高级认证代理商上海区BEID

上海

上海众翔科技发展有限公司	allwin technology(shanghai)Co.，Ltd	上海
北京佳易恒瑞科技有限公司上海分公司	Beijing Jia Yi Heng Rui Technology Co.，Ltd.	上海
上海比蒙商用信息系统科技有限公司	Bimeng Information System Integration Co.， Ltd.	上海
上海翼虎信息技术有限公司	E-Tiger Information Technology (Shanghai) CO，.LTD	上海
宏音飞翼信息科技(上海)有限公司	eWings Technologies，Inc.	上海
新电信息科技苏州有限公司上海分公司	NCS Information Technology(Suzhou)Co Ltd	上海
正音科技（上海）有限公司	RightCall Technologies Co.， Ltd.	上海
上海广瀚信息技术有限公司	Shanghai GuangHan Information Technology Co.，Ltd	上海
上海国腾致瑞科技有限公司	shanghai guoteng zhirui technonogy Co.	上海
上海浩然网络通讯设备有限公司	SHANGHAI HAORAN NETWORK DEVICES LTD	上海
上海理想信息产业（集团）有限公司	Shanghai Ideal Information Industry (Group) Co.， Ltd.	上海

上海交大慧谷信息产业股份有限公司	shanghai jiaoda withub information industrial Co.，Ltd.	上海
上海兰恒信息系统有限公司	Shanghai Lanheng Information System co; Ltd	上海
上海蓝蔚科技发展有限公司	SHANGHAI LANWAN TECHNOLOGY DEVELOPMENT CO.，LTD.	上海
上海明扬计算机科技有限公司	Shanghai Ming Yang Computer Technology Co.，Ltd.	上海
上海明羽实业有限公司	Shanghai Mingyu Industry Co.，Ltd.	上海
上海南康科技有限公司	Shanghai Nankang S&T Co.，Ltd.	上海
上海衍方信息技术有限公司	SHANGHAI YAN FANG TECHNOLOGIES	上海
上海今日在线科技发展有限公司	TODAY &TECHNOLOGY DEVELOPMENT CO.， LTD	上海
上海盈望信息技术有限公司	WIN LEGEND TECHNOLOGY CO LTD	上海
上海信申信息技术有限公司	XINSHEN TECHNOLOGY&INFORMATION CO LTD	上海

查询高级认证代理商北区BEID

北区

内蒙古亨达海天网络技术有限公司	Inner Mongloia Hengdahaitian Network Technical Co.，Ltd	包头
内蒙古天地方正信息有限责任公司	InnerMonglia TiandiFounder Information CO.，LTD	呼和浩特
内蒙古灵奕（集团）信息技术有限责任公司	Neimenggu Lingyi Information Technology Co.，Ltd	呼和浩特
内蒙古天迅网络技术有限公司	NEIMENGGU TIANXUN NETWORK CO.，LTD	呼和浩特
内蒙古万德系统集成有限责任公司	INNER MONGOLIA WIDE	呼和浩特

	SYSTEM INTEGRATION LTD.	
哈尔滨中太科技发展有限公司	HARBIN JOTAI SEINICE & TECHNOLOGY CO LTD	哈尔滨
哈尔滨市世纪大恒科技发展有限公司	HARBIN SHIJI DAHENG TECHNOLOGY DEVELOPMENT CO	哈尔滨
大连运邦科技发展有限公司	BRIDGE COMPUTER & COMMUNICATION CO.，LTD.	大连
大连宏旗计算机网络技术发展有限公司	DaLian HongQi Computer Network Co.Ltd	大连
大连正德信息技术发展有限公司	DALIAN ZHENGDE ELECTION CO LTD	大连
天津先进信息产品有限公司	Tianjin Advanced Information Products Co.，Ltd	天津
天津市爱德科技发展有限公司	Tianjin Aide Science Development Co.，Ltd	天津
天津市鼎泰科技发展有限公司	Tianjin digital tide technology development Co.，Ltd	天津
天津市远辰科技发展有限公司	Tianjin Fortune Science &Technology Development Co.Ltd.	天津
天津市方卫信息系统工程技术有限公司	TIANJIN FOUNDER WAY INFOSYSTEM TECHCO	天津
天津腾梁科技发展有限公司	TIANJIN TECH-LINK SCIENCE & DEVELOPMENT INC	天津
天津天地伟业科技有限公司	Tianjin Tiandy Tech.Co.，Ltd	天津
天津市英环信诚科技有限公司	TIANJIN YINGHUAN DATA EQUIPMENT CO LTD	天津
天津中环华迪计算机网络设备有限公司	Tianjin Zhonghuan Huadi Computer Network Device Co.，Ltd	天津
天津市奥拓电脑网络系统集成公司	AUTO COMPUTER & NETWORK SYSTEM	天津

	CO.，LTD	
天津开发区先特网络系统有限公司	TIANJIN EXPLOITATION DISTRICT FASTNET NETWORK	天津
山西同昌信息技术实业有限公司	SHANXI TOPCHANCE INFORMATION TECHNOLOGY INDUSTRIAL CO.LTD	太原
山西清华网络系统工程有限公司	Shanxi TsingHua Network System Engineering Company Ltd.	太原
太原市畅网科技发展有限公司	TaiYuan Orientent Development Co.， Ltd.	太原
沈阳易联科技有限公司	SHENYANG COMBINE TECHNOLOGY Co.，LTD	沈阳
沈阳福海达科技有限公司	Shenyang FuHaiDa Technology Co.，Ltd	沈阳
沈阳新金山电子技术有限公司	SHENYANG XIN GOLDEN MOUNTAIN ELECTRIC TECH CO	沈阳
济南森特电子有限责任公司	JiNan SENTE ELELTRON CO.LTD	济南
济南易盛伟业科技有限公司	jinan yishengweiye technology co.， ltd	济南
鲁能网络信息有限公司	LUNENG INFORMATION & NETWORK CO.LTD	济南
山东天南科技发展有限公司	shan dong tian nan technology development co.，ltd	济南
潍坊升华信息网络有限公司	WEIFANG SHENGHUA INFORMATION NETWORK CO.，LTD	潍坊
河北万方中天科技有限公司	Hebei Wanfang-zhongtian Science-Tech Co.，LTD	石家庄
河北普瑞电子有限公司	PRIME ELECTRONICS CO LTD	石家庄
石家庄博士林科技开发有限公司	Shijiazhuang Brilliance Science&Tech. Development	石家庄

	Co.，Ltd.	
河南省宇达科技有限公司	henan yuda technology co.，ltd	郑州
郑州创元计算机网络工程有限公司	CREAT NETWORKING SYSTEM ENGINEERING CO LTD	郑州
鄂尔多斯市创智电子公司	NEIMENGGU CHUANGZHI ELEC CO.，LTD	鄂尔多斯
吉林中软吉大信息技术有限公司	JILIN CSS&JLU INFO-TECH CO LTD	长春
青岛诺亚信息技术有限公司	Noah IT Co.，Ltd	青岛
青岛世纪黄河电子工程有限公司	Qingdao Huanghe Electronic System Co.，Ltd.	青岛
青岛蓝拓信息科技有限公司	Qingdao Lantop Information Tech Co.，Ltd	青岛
青岛鑫雷音电子有限公司	xinleiyin electron Ltd. qingdao (CHINA)	青岛

查询高级认证代理商东区BEID

东北

江西汇天科技有限公司	Jiangxi huitian technology co.ltd	南昌
江西海星计算机系统集成有限公司	JIANGXI SEASTAR COMPUTER SYSTEM INTEGRATION C	南昌
江西思创数码科技有限公司	JIANGXI STRONG HIGH TECHNOLOGY CO.，LTD.	南昌
江西贝尔科技产业有限公司	JIANGXI BELL TECHNOLOGY INDUSTRY CO.LTD.	南昌
宁波北宇科技发展有限公司	Bestward Technology Development Co.，Ltd Of Ningbo	宁波
宁波江北华力电脑有限公司	Ningbo jiangbei huali computer	宁波

	co.，Ltd	
杭州城讯信息技术有限公司	hangzhou chengxun information technology co.，ltd.	杭州
杭州时代银通计算机工程有限公司	HANGZHOU ERAYINTONG COMPUTER ENGINEERING CO.，LTD.	杭州
杭州冠恒计算机网络有限公司	hangzhou guanheng computer network co.，LTD	杭州
杭州新世纪信息技术有限公司	Hangzhou New Century Information System Engineering Co.，Ltd	杭州
杭州通裕通信科技有限公司	HANGZHOU TONY COMMUNICATION LTD	杭州
UT斯达康通讯有限公司	UTStarcom Telcom	杭州
浙江爱特科技有限公司	Zhejiang ActiveTech Computer Technology Co.Ltd.	杭州
浙江创联信息技术股份有限公司	ZHEJIANG CREA-UNION SOFTWARE CO LTD	杭州
武汉烽火信息集成技术有限公司	Fiberhome Integration Technologies Co.，Ltd	武汉
湖北公众信息产业有限责任公司	Hubei Public Information Industry Co.，Ltd	武汉
武汉万联数据通信系统工程有限公司	WANLINK DATACOMM SYSTEM ENGINEERING LTD	武汉
武汉钢铁工程技术集团自动化有限责任公司	WISET Automation Co.，LTD	武汉
武汉保全科技有限公司	Wuhan Bao Quan Services CO.，Ltd.	武汉
武汉蓝星科技股份有限公司	WUHAN BLUEGRID TECHNOLOGY CO. LTD	武汉
武汉数字工程研究所	WUHAN DIGITAL ENGINEERING INSTITUTE	武汉
武汉奔腾网络系统集成有限公司	WUHAN SPEEDNET SYSTEM INTEGRATION CO LTD	武汉
武汉市天宝网络工程有限公司	WUHAN TIAN BAO NETWORK PROJECT	武汉

	CO.，LTD	
武汉兴得科技有限公司	Wuhan Xingde Science&Technology Co.，LTD	武汉
武汉通威电子有限公司	wuhantowaytech	武汉
武汉市蓝牙网络技术有限公司	WUHAN BLUEBUD NETWORK CO LTD	武汉
武汉广通系统工程有限公司	WUHAN GOTOP SYSTEMS ENGINEERING CO.， LTD.	武汉
武汉菲旺软件技术有限责任公司	WUHAN PHILWONG COMPUTER TECHNOLOGY CO.，LTD.	武汉
江苏晨网软件有限公司	JIANGSU CHAINNET SOFT CO.，LTD	南京
江苏省宏图电子综合研究所有限公司	Jiangsu Hongtu Electronic Research Institute Co.，Ltd.	南京
南京安瑞诺文信息技术有限公司	NANJING ARROW-NOW INFORMATION TECHNOLOGY CO.， LTD	南京
南京科融数据系统有限公司	NANJING FITECH DATA SYSTEM CO LTD	南京
南京迈康网络技术有限公司	Nanjing Maikang Networks Technology Co.	南京
南京苏得控制系统有限公司	NanJing Sude Control System CO.，LTD	南京
南京泰融科技发展有限公司	Nanjing Tairong Technology Co.，Ltd	南京
南京银淼数码科技有限公司	NanJing Yinmiao Digital technoiogy Go.，Ltd	南京
苏源集团江苏信息技术有限公司	SuYuan Group Jiangsu Information Technology CO.，Ltd	南京
南京鼎盟科技有限公司	TOPTEAM INFO CO LTD	南京
江苏宏图高科技术开发有限公司	JIANGSU HONGTU HI-TECHNOLOGY DEVELOPMENT CO.LTD	南京

安徽中科大讯飞信息科技有限公司	ANHUI USTC IFLYTEK INFORMATION TECH CO LTD	合肥
徐州市联众创科电子工程有限公司	Unitehuman create technology electronic project co.，ltd	徐州
无锡快威网络科技有限公司	WuXi KaWay Networks Technoligy Co.，Ltd	无锡
无锡乾初科技有限公司	Wuxi Qianchu Science and Technology Co.， Ltd.	无锡
苏州南大苏富特科技有限公司	suzhou nandasoft CO.，LTD	苏州
苏州工业园区纵横计算机有限公司	Suzhou New Horizon Computer Co.， Ltd	苏州
苏州新众友信息科技有限公司	SUZHOU TRUE COMPUTER SYSTEM ENGINE CO.，LTD.	苏州

查询高级认证代理商南区BEID

南区

广西宝亮升维网络科技有限公司	NANNING SUNWAY TECHNOLOGY ENGINEERING CO LTD	南宁
实达科技(福建)软件系统集团有限公司	START-TECH(FUJIAN) SOFTWARE & SYSTEM CO.，LTD	厦门
厦门柏事特信息科技有限公司	XIA MEN Best Information Technology Co.，Ltd	厦门
厦门市金利得电子科技有限公司	Xia Men Gold Leader Electronic Scientech Co. Ltd	厦门
厦门伊网通数码科技有限公司	Xiamen E-enet Digital Technology Co.，LTD.	厦门
厦门东南融通系统工程有限公司	Xiamen Longtop System Co.， Ltd.	厦门
厦门至精诚系统集成公司	Xiamen P&S Computer System Integrated Co.，Ltd	厦门
厦门创思信息技术有限公司	XIAMEN TRUST INFORMATION TECH CO.，LTD	厦门

厦门维思信息产业有限公司	XIAMEN WINS INFORMATION INDUSTRIAL	厦门
厦门纵横集团科技股份有限公司	Xiamen Zongheng Group Science & Technology Co.，Ltd	厦门
厦门天同系统工程有限公司	XIAXIN ADVANCED SYSTEMS CO LTD	厦门
安迅(广州)科技服务有限公司	NCR (Guangzhou) Technology Services Limited	广州
广东数据通信网络有限公司	GUANGDONG DATA COMMUNICATIONS NETWORK COLTD	广州
广州市奔瀛计算机科技有限公司	GuangZhou Benying Technology Company limited	广州
广州冠亚科技有限公司	Guangzhou Crest Technology CO.，LTD.	广州
广州中软信息技术有限公司	Guangzhou CS&S Information Technology Co.，Ltd	广州
广州翼风通信技术有限公司	GuangZhou E-Wind Communication Technology Ltd.	广州
广州市共能资讯科技有限公司	Guangzhou ITShare Technology Co.，ltd.	广州
广州金鹏集团有限公司	GuangZhou JinPeng Group BeiJing branch	广州
广州市康汇数码科技有限公司	Guangzhou Kang Hui Digital Technology CO.， LTD	广州
广州市康谱达电子科技有限公司	Guangzhou KPD technology Co.Ltd.	广州
广州市尚阳电子科技有限公司	Guangzhou Shangyang Electronic Technology Co.，Ltd	广州
广州锐欣科技有限公司	Guangzhou Sinogtid Technology	广州
广州中铁信息工程有限公司	Guangzhou SinoRails Hong Kang Computer Co.，Ltd	广州
广州市南鹰计算机有限公司	guangzhou south eagle computer co，ltd	广州
广州创逊数据系统有限公司	Guangzhou Strengthen Data System Co.， LTD	广州
广州阳光耐特电子有限公司	GuangZhou YangGuang Naite Elec	广州

	Co.，Ltd	
广州市恒讯科技有限公司	HANSSUN	广州
广州胡仕网络科技有限公司	HuShi Network Technology(Guangzhou) Co.，Ltd	广州
金鹏电子信息机器有限公司	Jinpeng Electronic Information Machine Co.，Ltd.	广州
广州怡和科技工程有限公司	JOS Technology (Guangzhou) Co.，Ltd.	广州
广州市富思信息技术有限公司	NETLAND COMPUTER SYSTEM CO LTD	广州
广州先一数码科技有限公司	Precede Digit(GZ)CO.，LTD	广州
惠州英诺信息技术有限公司	Innovation information Technology Inc	惠州
广东宏景科技有限公司	GLORY VIEW TECHNOLOGY CO.，LTD.SHANTOU	汕头
广东蓝凌科技有限公司	LANDRAY INFORMATION TECHNOLOGY CO LTD	汕头
汕头市集铭网络技术有限公司	SHANTOU GEMMY NETWORK CO.LTD	汕头
海口联合华远电脑网络有限公司	Haikou Lianhehuayuan Computer Network Co.， Ltd.	海口
海南大有计算机有限公司	hainan dayou computer CO.，LTD	海口
海南海容网络技术有限公司	Hainan Hairong Computer&Network Co.，Ltd	海口
海南兆纬信息产业有限公司	HAINAN JOINWAY INFORMATION INDUSTRY CO LTD	海口
海南海航航空信息系统有限公司	HNA SYSTEMS CO.，LTD.	海口
深圳市科健信息技术有限公司	Shenzhen Kejian Info-tech Co.，Ltd.	深圳
深圳市康帕斯科技	COMPASS TECHNOLOGY	深圳
深圳市爱华通用电脑有限公司	Shenzhen Aiwa Common Computer Co.， Ltd	深圳
深圳市脉山龙信息技术股份有限公司	SHENZHEN BAY-LAB CO.，LTD.	深圳

深圳市数据建设有限公司	shenzhen data system co.，Ltd	深圳
深圳市亿蓝科技有限公司	SHENZHEN ELINE TECHNOLOGIES CO.，LTD.	深圳
深圳市天才坊实业有限公司	shenzhen Googhelper Industry Co.，Ltd	深圳
深圳华强信息产业有限公司	SHENZHEN HUAQIANG INFORMATION INDUSTRY CO.，LTD.	深圳
深圳智宇实业发展有限公司	SHENZHEN IB TECHNOLOGIES DEVELOPMENT CO.，LD	深圳
深圳市杰迪讯科技有限公司	SHENZHEN JEDISUN TECHONLOGY CO.，LTD.	深圳
深圳市金证科技股份有限公司	Shenzhen Kingstar Technology Co.	深圳
深圳市新链路电子有限公司	SHENZHEN NEWNET ELECTRONICS CO LTD	深圳
深圳市天舟网络通信有限公司	SHENZHEN SKYNET COMMUNICATION CO.，LTD	深圳
深圳市旭感和成信息技术有限公司	SHENZHEN SYSCAN DIGITAL SYSTEMS CO.，LTD	深圳
深圳市天地和网络有限公司	shenzhen tiandihe network co.，ltd Fax_Region	深圳
深圳市通盛网络技术有限公司	SHENZHEN TONTION NETWORKING TECHNOLOGY CO.， LTD	深圳
深圳市联合信息科技发展有限公司	SHENZHEN UNION INFOMATION TECHNOLOGY CO.，LTD.	深圳
深圳市维新康实业有限公司	SHENZHEN WINSCOM INDUSTRIAL & DEVELOPMENT CO	深圳
深圳市欣兰网科技发展有限公司	Shenzhen Xinlan Networking Technology Co.，Ltd	深圳
深圳市鑫同航电子有限公司	SHENZHEN XINTONGHANG ELECTRONIC CO LTD	深圳
深圳银兴科技开发有限公司	Shenzhen Yinxing Science &Technology Development Co.，Ltd	深圳

深圳市烁迪科技有限公司	shenzhenshuodi technology co.，ltd.	深圳
通国科技(深圳)有限公司	TCS TECHNOLOGY (SHEN ZHEN) CO.，LTD	深圳
深圳市南凌科技发展有限公司	SHENZHEN NOVA TECHNOLOGIES DEVELOPMENT CO.， LTD.	深圳
福州长威网络科技有限公司	EVECOM NETWORKS CO LTD	福州
福建北佳信息技术有限公司	Fujian BeiJia Information Technology CO LTD	福州
福建恒锋电子有限公司	Fujian Hengfeng electric Co.， LTD.	福州
福建新大陆电脑股份有限公司	FUJIAN NEWLAND COMPUTER CO.，LTD	福州
福州康联科技发展有限公司	FUZHOU COMLINK TECHNOLOGY DEVELOPMENT CO LTD	福州
福建泰讯网络科技有限公司	Telthink Network Technologies Co.，Ltd	福州
福建优普科技有限公司	FUJIAN UPLIFE INFORMATION TECHNOLOGY CO	福州
长沙科创计算机系统集成有限公司	CHANGSHA CREATOR SYSTEM INTEGRATION CO.LTD	长沙
湖南创骏网络技术公司	Hunan Chuangjun Network Technical Company Ltd.	长沙
湖南电子信息产业集团有限公司	Hunan Electrnic Information Industry Group Company，LTD	长沙
湖南科诚科技发展有限公司	Hunan Kecheng H-Tech Deve.Co.Ltd.	长沙
湖南拓维信息系统股份有限公司	TALKWEB INFORMATION SYSTEM CO.，LTD	长沙

查询高级认证代理商西区BEID

西区

广西宝亮升维网络科技有限公司	NANNING SUNWAY TECHNOLOGY ENGINEERING CO LTD	南宁

实达科技(福建)软件系统集团有限公司	START-TECH(FUJIAN) SOFTWARE & SYSTEM CO.，LTD	厦门
厦门柏事特信息科技有限公司	XIA MEN Best Information Technology Co.，Ltd	厦门
厦门市金利得电子科技有限公司	Xia Men Gold Leader Electronic Scientech Co. Ltd	厦门
厦门伊网通数码科技有限公司	Xiamen E-enet Digital Technology Co.，LTD.	厦门
厦门东南融通系统工程有限公司	Xiamen Longtop System Co.， Ltd.	厦门
厦门至精诚系统集成公司	Xiamen P&S Computer System Integrated Co.，Ltd	厦门
厦门创思信息技术有限公司	XIAMEN TRUST INFORMATION TECH CO.，LTD	厦门
厦门维思信息产业有限公司	XIAMEN WINS INFORMATION INDUSTRIAL	厦门
厦门纵横集团科技股份有限公司	Xiamen Zongheng Group Science & Technology Co.，Ltd	厦门
厦门天同系统工程有限公司	XIAXIN ADVANCED SYSTEMS CO LTD	厦门
安迅(广州)科技服务有限公司	NCR (Guangzhou) Technology Services Limited	广州
甘肃金融电脑公司	GANSU FINANCE COMPUTER CO	兰州
甘肃金桥通信技术有限公司	GANSU JINQIAO COMMUNICATION TECHNOLOGY CO.，LTD	兰州
甘肃浪潮电子工程有限公司	Gansu Langchao Electronic Engneering Co.Ltd	兰州
甘肃森智信息产业有限责任公司	Gansu SenZhi information industry co.，LTD	兰州
甘肃万维信息技术有限责任公司	GANSU WANWEI MULTMEDIA INFORMATION CO.， LTD.	兰州
甘肃新网通科技信息有限公司	Gansu Xinwangtong Science and Technology Information	兰州
兰州飞天网景信息产业有限公司	Lanzhou Feitian Netscape Information Industry Co.，Ltd	兰州

兰州海星科技有限责任公司	LanZhou Seastar Scien-tech Ltd	兰州
兰州星耀网络信息有限责任公司	lanzhou starnet info-tech co.ltd	兰州
成都伊地商贸有限公司	Cheng Du Yi Di Trade Co.，Ltd.	成都
成都三零盛安信息系统有限公司	CHENGDU 30SAN INFORMATION SYSTEM CO.，LTD	成都
成都安托系统集成有限公司	ChengDu ATOZ Systems Integration Limited	成都
成都金电科技有限责任公司	ChengDu FEST co-operation limited	成都
成都恒泰科技发展有限公司	ChengDu HengTai Science And Technology Development CO.，LTD	成都
成都九联网络科技有限公司	Chengdu Joinnet Networks Technology Co.Ltd FaxRegion	成都
成都精通网络技术有限公司	Chengdu Kingcom Network Technology Co.，Ltd.	成都
成都联鑫信息网络有限公司	CHENGDU LANSYSTEM INFORMATION NET CO LTD	成都
成都美福捷瑞信息咨询有限公司	Chengdu MFGR Information Consultation Co，.Ltd.	成都
成都兰深电子有限公司	Chengdu Nanscent Electron Co.，Ltd	成都
成都全码科技有限公司	Chengdu Quanma Technology Co.，Ltd.	成都
成都瑞克耐特科技有限公司	Chengdu Recordnet Technoloiges Ltd.	成都
成都思蓝网络有限公司	CHENGDU SILAN NETWORKING TECHNOLOGY CO.，LTD	成都
成都星网璟科技有限公司	ChengDu xing Wang Jing Technology Co.，Ltd	成都
成都优派科技实业有限公司	CHENGDU YOUPAI TECH.CO. LTD	成都
成都市鑫阳光信息系统有限责任公司	CHENGDUSHI XIN-SUNNY INFORMATION SYSTEM CO.LTD	成都
吉虎系统科技有限责任公司	Gecko system technology co.，Ltd	成都
兴迪资讯科技有限公司	New Design Information Technology Co.，Ltd.	成都
四川省东方惠群科技发展有限公司	ontelsoft(si chuan)co.，Ltd.	成都

四川省天财网络有限责任公司	Sichuan tiancai netwaork co.，ltd	成都
四川新迎顺信息技术有限公司	sichuan xinyingshun information technology co.，ltd	成都
成都赛恩计算机网络技术有限公司	CHENGDU SIGN COMPUTER NETWORKING CO LTD	成都
成都泽鑫电脑网络有限责任公司	CHENGDU ZEXIN COMPUTER NETWORK CO LTD	成都
四川博世科技信息产业有限公司	Sichuan Boss Technology Information Industry Co.，Ltd.	成都
四川华胜信息产业有限责任公司	SICHUAN HUASHENG INFORMATION INDUSTRY COLTD	成都
四川省创意技术发展有限责任公司	SICHUAN TROY TECNOLOGY DEVELOPMENT COLTD	成都
云南爱迪科技有限公司	KUNMING AIDI SCIENCE TECHNOLOGY DEVELOPMENT CO.，LTD.	昆明
昆明必安网络数码有限责任公司	kunming bi'an digital co.，ltd	昆明
昆明恩捷科技有限公司	kunming enjie technology ltd，.co	昆明
昆明冠豪科技有限公司	Kunming GuanHao Science and Technology CO.Ltd	昆明
昆明英特格科技有限公司	KunMing Integer Technology Co.，Ltd	昆明
昆明龙志达工贸有限公司	kunming longzhida industry commerce co，.ltd	昆明
昆明优力威尔信息系统有限公司	Kunming Uniwell Information System Inc.	昆明
云南博鸣科技开发有限公司	yunnan Boming technology exploitation co.，ltd	昆明
云南万峰信息产业有限公司	YUNNAN WANFENG INFORMATION TECH COLTD	昆明
西宁得晖科技贸易有限责任公司	XiNing DeHui technology commerce Co.，Ltd	西宁
陕西金叶西工大软件股份有限公司	SHAANXI GLNPU SOFTWARE CO.，LTD	西安
陕西瑞金电子科技有限公司	SHAANXI RUIJIN ELECTRON TECHNOLOGY	西安

陕西深思科技企业有限公司	SHANXI SNSI TECHNOLOGY CO LTD	西安
西安爱必克电子技术有限公司	xi'an IBC electrical technology co.，ltd	西安
西安合强数码有限公司	XIAN UNIWAY DIGITAL CO LTD	西安
贵州联益科技发展有限公司	Guizhou Co-profit Technology Development Co.，LTD	贵阳
贵州九阳网络科技有限公司	GUIZHOU ENJOY SCIENCE&TECHNOLOGY NETWORK CO	贵阳
贵州天讯信息产业有限公司	GUIZHOU TIANXUN INFORMATION INDUSTRY CO.;LTD	贵阳
贵州通联科技有限责任公司	GUIZHOU TONGLIAN TECHNOLOGY CO??????LTD	贵阳
贵州维讯信息技术有限公司	Guizhou Vision-IT Ltd.， Co.	贵阳
重庆南华中天信息技术有限公司	CHONG QING ZENITH COMPANY LTD	重庆
重庆长安信息科技股份有限公司	CHONGQING CHANGAN INFORMATION TECHNOLOGY CO.，LTD.	重庆
重庆汉光电子工程有限责任公司	CHONGQING HANGUANG ELECTRONIC ENGINEERING CO，LTD	重庆
重庆亚德科技有限责任公司	YADE SCIENCE & TECHOLOGY CO LTD	重庆
重庆怡讯网络技术有限公司	CHONGQING ECOM NETWORKS CO	重庆
重庆市易联数码科技有限公司	CHONGQING ELANE DIGITAL CO LTD	重庆
宁夏诚威伟业科技有限公司	Ningxia Chengweiweiye Technology Co.， Ltd.	银川

Addendum 2 to Question #1 – Cisco Networking Academies in China

This information is also available at:
http://locators.netacad.net/cnams/locators/AcademyClassLocator.jsp

China participating academies

Acad Id	Academy Name	City
1414	Network & Information Engineering Centre, Fudan University	Shanghai

5179	Tongji University	Shanghai
5216	Southeast University	Nanjing
5220	Northeastern University	Shenyang
5261	Huazhong University of Science and Technology	Wuhan
5262	South China University of Technology	Guangzhou
5401	University of Electronic Science & Technology of China	Chengdu
5402	Tsinghua University	Beijing
5403	Beijing University of Posts and Telecommunications	Beijing
5404	Zhongshan University	Guangzhou
5405	Shanghai Jiao Tong University	Shanghai
5406	Xian Jiaotong University	Xian
5407	Peking University	Beijing
5907	Chong Qing University	Chongqing
7454	Computer Information and Network Center of Tianjin University	Tianjin
9900	Northeast Agricultural University	Harbin
9960	Harbin Normal University	Harbin
13621	North China University of Technology	Beijing
13623	University of Science & Technology Beijing (Guanzhuang)	Beijing
13741	Beijing Information Technology Institute	Beijing
14955	Kunming University of Science and Technology	Kunming
17214	Agricultural University of Hebei	Baoding
22787	China Women's College	Beijing
22987	Communication University of China	Beijing
23007	Tai Yuan University of Technology	Taiyuan
24287	Shanxi University	Taiyuan
24307	China University of Science-Technology and Management	Beijing
24612	Inner Mongolia Polytechnic University	Huhhot
24613	Inner Mongolia Agricultural University	Huhhot
24614	Sichuan University	Chengdu
24640	Northwest Sci-Tech University of Agriculture and Forestry	Yangling
25427	Guangxi University	Nanning
25467	Southwest Forest College	Kunming
25468	Yunnan University	Kunming
25469	Yunnan Normal University	Kunming
25470	ChongQing University of Post and Telecom	Chongqing
27067	Gansu University of Technology	Lanzhou
27087	Ning Xia University	Yinchuan
27107	Qinghai University	Xining
27127	Xinjiang Petroleum Institute Network Center	urumqi
29367	Pui Ching Commercial College	Guangzhou
29464	Southwest JiaoTong University	Chengdu
31052	Tianjin Commercial Univ.	Tianjin
31053	Tianjin Polytechnic Univ.	Tianjin
31273	Tianjin Agricultural College	Tianjin
31275	Tianjin XinHua Employee Univ.	Tianjin
31888	Shanxi tushuguan technology tranning school	Xi'an
31889	College of Information Science, Beijing Normal University	Beijing
32778	UESTC Network Center	Chengdu
34172	Beijing Telecom School	Beijing
36248	Dalian Neusoft Institute of Information Technology	Dalian
36672	Inner Mongolia University	Huhhot
36729	Wenzhou University	Wenzhou
36761	Shenyang Institute of Technology	Shenyang
36857	Anhui University Cisco Network Academy	Hefei
36858	North University of China	Taiyuan
37022	Kunming University	Kunming
37109	Electronic Lab, Zhejiang University	Hangzhou

38210	Network Center of the Zhengzhou University	Zhengzhou
38211	Hebei University of Science and Technology	Shijiazhuang
38213	Hebei Normal University	Shijiazhuang
38215	Shanxi Teachers University	Linfen
38273	Tianjin Shiyan Huaguan School	Tianjin
38274	Shi Yan High School	Tianjin
38543	ShanDong University	Jinan
38560	Information School of Shandong University of Science & Technology	Taian
39053	ShenYang University	Shenyang
39054	LiaoNing University	Shenyang
39056	ShenYang University of Technology	Shenyang
39060	North-East Finance and Economic University(DaLian)	Dalian
39061	DaLian Institute of Light Industry	Dalian
39986	Shanghai Telecommunication Training Center	Shanghai
40946	Information Engineering Research Center of Nanchang University	Nanchang
40973	Southwest University of Science and Technology	Mianyang
41259	Nanjing University of Technology	Nanjing
41265	China University of Mining and Technology	Xuzhou
41266	Huai Hai Institute of Technology	Lianyungang
41485	Beijing University of Chemical Technology	Beijing
41885	School of Computer and Information Technology, Northern JiaoTong University	Beijing
42106	Beijing University of Technology	Beijing
42545	Cisco-Fudan Networking Academy Hainan local Academy	Haikou
43346	Northwest Normal University	Lanzhou
43535	Shenzhen Polytechnic	Shenzhen
49567	JiLin University	Changchun
50440	Central South University	Changsha
51163	Baotou University of Iron &Steel Technology	Baotou
51165	Chengdu University of Information Technology	Chengdu
51216	Sichuan University of Science and Technology	Chengdu
51223	Yanbian University	Yanji
51229	Chengdu University	Chengdu
51339	Guangzhou Civil Aviation College	Guangzhou
51340	Civil Aviation University of China	Tianjin
51868	SiChuan Electronic and Technical School	Guangyuan
52597	Guilin Institute of Electronic Technology	Guilin
52598	Dongguan Institute of Technology	Dongguan
52912	Fudan University Local Academy In Wuxi	Wuxi
53218	zhejiang university of technology	Hangzhou
53613	Zhejiang Institute of Mechanical & Electrical Engineering	Hangzhou
53614	Lanzhou Railway Institute	Lanzhou
3001373	Jimei University	Xiamen
3001457	Software School of Nanjing University	Nanjing
3001796	xian institute of posts & telecoms	Xi'an
3002116	Harbin Engineering University Automation College	Harbin
3002117	Institute of Technology, Tongji University	Shanghai
3002897	ShenYang Institute of Technology	Shenyang
3002898	Guangdong Provincial Institute for Technical Personnel(Zhuhai Campus)	Zhuhai
3002980	Software College of Fudan University	Shanghai
3003681	Ningbo College	Ningbo
3004739	Dalian University of Technology	Dalian
3005560	Xidian University	Xi'an
3006405	Shandong University of Technology	Zibo
3006406	East China University of Science and Technology	Shanghai
3006407	Hangzhou Vocational Technology College	Hangzhou
3006408	Xu Zhou Normal University Computer Engineer Department	Xuzhou
3006411	Xu Zhou Radio and TV University Machinery Branch	Xuzhou

3006603	Anshan University of Science and Technology	Anshan
3008491	Huhhot Networking technology training School	Huhhot
3008492	Yantai Qingquan School	Yantai
3008494	SHI JIA ZHUANG UNIVERSITY of CEONOMICS	Shijiazhuang
3008527	Hubei automotive industries institute	Shiyan
3008549	University of Petroleum (Eastern China)	Dongying
3008586	Nanyang Institute of Technology	Nanyang
3008587	Jianghan University	Wuhan
3008588	Jiangxi Agricultural University	Nanchang
3008589	Xi Bei University	Xi'an
3008591	Zhejiang Forestry University	Linan
3008592	Minjiang University Software Engineering Insititute	Fuzhou
3008686	Jinan University	Jinan
3008688	West Anhui University	Liuan
3008689	Nantong Textile Vocational Technology College	Nantong
3008908	Zhejiang Normal University	Jinhua
3008909	Peking University Founder College	Langfang
3011588	Suzhou Industrial Park Institute of Vocational	Suzhou
3012012	Jilin Railway Economic Institute	Jilin
3012188	Hangzhou State Software Industry Base	Hangzhou
3012189	Ningbo University	Ningbo
3012346	Henan Information Engineering College	Zhengzhou
3012348	Wujiang Vocational Technology College	Wujiang
3012680	MOS Software Institute of East China Technology Institute	Nanchang
3012683	East China Jiaotong University	Nanchang
3012740	Software College of NorthWestern Polytechnical University	Xi'an
3012799	China Agricultural University	Beijing
3012860	South Western University of Finance and Economics	Chengdu
3012998	Northeast Agricaltural University	Haerbin
3013037	Software College of Beijing University of Technology	Beijing
3013359	Hebei Software Institute	Baoding
3014060	Tianjin Manager Academy	Tianjin
3014119	Xi'an University of Architecture and Technology	Xi'an
3014619	Chuzhou University	Chuzhou
3014620	Changzhou College of Information Technology	Changzhou
3014698	Fuzhou University	fuzhou
3014699	Heilongjiang August First Land Reclaimation University	daqing
3014700	Zhejiang Wanli University	ningbo
3014898	Zhuhai College of Beijing Normal University	Zhuhai
3014899	Guangxi Radio & TV University	nanning
3014919	Nanjing -tic	NANJING
3015146	Changchun University of Technology	Changchun
3015148	Liaoning Police Officer College	Dalian
3015168	Harbin Hua Xia Computer Professional College	Harbin
3015220	Inner Mongolia Electron Info Employment Technology Seminary	Huhot
3015221	Nanning No. 1 Secondary Vocational School	Nanning
3015222	Anhui Industry Polytechnic	Tongling
3015238	Information College of Zhejiang Normal University	Jinhua
3015244	No. 6 Secondary Vocational School	Nanning
3015245	Guangxi Hydraulic and Electric Polytechnic	Nanning
3015340	Sichuan TOP Vocational College of Information Technology	chengdu
3015341	Sijiazhuang No. 3 Vocational School	shijiazhuang
3016919	Network and Information center, Beijing City University	Beijing
3016920	Dept. of Network Engineering,Chengdu Univ. of information tech.	Chengdu
3016921	Network Center of Ocean University of China	Qingdao
3016922	Cheng Du Neusoft Institute Information Technology	Chengdu
3017123	Jiangxi vocational college of finance and economics	Jiujiang

3017125	Shangrao Normal College(SRNC)	shaorao
3017759	Computer and Information Engineering Department,Yantai Vocational College	Yantai
3017760	Shandong College of Art & Design Network Information Center	Jinan
3017761	Department of Computer Science Beijing Institute of Graphic Communication	Beijing
3018160	GuangDong ZhuHai No.3 Middle Vocational School	zhuhai
3018161	School of engineer of changchun university of technology	changchun
3018162	Guangxi Technological college Of machinery and Electricity	Nanning
3018163	Anhui Wenda Information Technology College	Heifei
3018164	Beijing Information Management School	Beijing
3018166	Shaoxing University Network Management Office	shaoxing
3018167	University of Science and Technology Beijing Information Engieering College	beijing
3018191	ChangChun University	changchun
3018223	School of Software of Dalian University of Technology	Dalian
3018439	Network Infor. Dep. Fengman Senior Technical Institute of Hydroelectric Power	Jilin
3018440	BEIJING INSTITUTE OF ECONOMIC MANAGEMENT	Beijing
3018583	Huangpu Vocational School	guangzhou
3020620	Baoding Technical College Of Electrc Power Information Department	Baoding
3020621	Changzhou Institute of Technology School of Computer & Information Engineering	Changzhou
3020622	Highway Transportation Science & Tech. Infor. Center Of Gansu Prov.	Lanzhou
3020623	GuangZhou University Network& Modern Education Technology Center	Guangzhou
3020624	Information Center_Deqiang Business College Harbin University of Commerce	Harbin
3020625	college of science, Huazhong Agricultural University	WuHan
3020626	LiaoCheng vocation and technology college Computer Department	Liaocheng
3020627	E-Information Department, Qingdao Harbor Vocational Technology College	Qingdao
3020628	Tianjin Huayuan Software Area Construction & Development Co.,Ltd	Tianjin
3020629	WuHan Institute of Shipbuilding Tech. Elec. & Elec. Engineering Dep.	Wuhan
3020630	wuhan software vocation college network center	Wuhan
3020631	Shihezi University Tech. & Infor. Collage	Shihezi
3020633	Jinan Railway Polytechnic	Jinan
3020634	Dept. of Computer Science, Qufu Normal University	Rizhao
3020676	The construction engineering college of Hebei Manage the profession	Zhangjiakou
3020677	Shanghai Tuopu Information Technical College	Shanghai
3020705	ZheJiang University Of Finace & Economics information college	Hangzhou
3021661	Heilongjiang G-bond Technical Training Center	harbin

RESPONSES FROM MR. JACK KRUMHOLTZ, MANAGING DIRECTOR OF FEDERAL GOVERNMENT AFFAIRS AND ASSOCIATE GENERAL COUNSEL, MICROSOFT CORPORATION, TO QUESTIONS SUBMITTED FOR THE RECORD BY THE HONORABLE CHRISTOPHER H. SMITH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY AND CHAIRMAN, SUBCOMMITTEE ON AFRICA, GLOBAL HUMAN RIGHTS AND INTERNATIONAL OPERATIONS, AND THE HONORABLE THOMAS G. TANCREDO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Question:

How many requests on a daily or weekly average does Microsoft Corporation receive to censor content, provide information about users, remove web logs, or update or fine tune filtering equipment?

Response:

All MSN users must agree to the MSN Terms of Use before using any of our services. We receive numerous requests to remove user-generated content that violates our terms of use, which prohibit using our services to incite, advocate, or express pornography, obscenity, vulgarity, profanity, hatred, bigotry, racism, or gratuitous violence, or to use our service in any way that is illegal or violates any local and national laws (e.g., the sale of Nazi paraphernalia in Germany, or the encouragement of terrorism in Spain). Some of these requests to remove content are from other customers who are offended by the content, and some requests are from governments. We require formal written notification from governments stating the legal basis for the request before we will remove user-generated content. In all cases, we verify that the content does violate our terms of use or local law before we remove the content. We also receive numerous requests from law enforcement for customer information related to criminal conduct on the Internet. We require a formal written request that is valid under governing local law stating the legal basis for the request and the nature of the investigation. To comply with requests for personal information, we require that the request be related to an ongoing investigation of a crime under the laws of the requesting country, and the United States; that is, we require a showing of "dual criminality", the same standard that is applied under China's Mutual Legal Assistance Agreement with the United States. We process these requests in full compliance with the Electronic Communications Privacy Act. If a request does not meet the requirements of the Electronic Communications Privacy Act, we reject it.

Question:

Describe the legal process by which Microsoft receives a request to censor or provide information, what documents does the government of China present and how specific are the documents?

Response:

As described above, with respect to China and all other countries, we require formal written notification stating the legal basis for a request to remove user-generated content or to provide customer information.

Question:

Describe the established procedures for handling Chinese requests for censorship of electronic information.

Response:

As described above, we require formal written notification stating the legal basis for the requests.

Question:

Are there requests for clarification?

Response:

We ask for the specific legal basis for the request, ie, the specific regulation that is violated by the content.

Question:

Are there automatic referrals to U.S. headquarters/legal counsel?

Response:

Counsel in China and in the United States are often involved in processing these requests.

Question:

Are there legal appeals?

Response:

We are not aware of any appellate process that is available under Chinese law. We are also not aware of any customer availing him or herself of such a procedure.

Question:

In what circumstances would Microsoft refuse a Chinese request?

Response:

We can't really speculate about what we would or would not do in a given circumstance. We require the Chinese government to provide us with a formal written notification stating the legal basis of the request, and we review that request for compliance with local law and our policy. As stated above, if the request fails to comply with the requirements of the Electronic Communications Privacy Act and our policy, we reject it.

Question:

Provide the list of words and web sites the PRC provides Microsoft with to censor or block access to electronic information.

Response:

We would prefer to discuss this answer with you or your staff in a confidential manner. We understand your interest and concern about what terms are treated in this manner, but for several reasons which we can elaborate, we think it is better not to make such lists public.

Question:

Has Microsoft been required by the government of China to censor information related to China's one-child policy?

Response:

No.

Question:

Is Microsoft depositing a long-term cookie on Chinese users' computers, if the computer is configured to accept cookies?

Response:

MSN uses cookies in our services in China just as we do in all other markets; there is nothing different about the use of cookies in China vs. other markets.

Question:

When do Microsoft cookies expire?

Response:

There are various lengths of cookie expirations; there is not one standard expiration term across Microsoft. As stated above, there is no special expiration term for Chinese users.

Question:

Is Microsoft logging user IP addresses?

Response:

Yes, as disclosed in our privacy statement, we do log Internet Protocol (IP) addresses. A standard part of web technology is to log IP addresses of visitors to a page or service. These are used by providers in a variety of ways, including troubleshooting network performance, providing customer support, or ensuring network security, such as to determine if a network intrusion or denial of service attack is taking place, and if so, the source of that attack.

Question:

Are user IP addresses matched to the Microsoft cookie, or can they be?

Response:

There are a variety of cookies set by different Internet services for different purposes, not one Microsoft cookie. Within the MSN and WindowsLive products, cookie information could be matched to IP address.

Question:

Are users' search terms logged by IP address?

Response:

As disclosed in our privacy statement, "Each time you use MSN Search, including the MSN Toolbar, cookies may be placed on your machine and MSN may collect your Internet IP address, the time and date of your search terms, and your browser configuration. MSN may use this information to customize your search results."

Question:

Are users' search terms logged by cookie ID?

Response:

The information collected in association with cookies, as described in the privacy statement language quoted in the prior answer, is associated with an anonymous ID for that cookie.

Question:

Can users' search terms be tied to either a cookie or an IP address?

Response:

Yes, users' search terms can be tied to an anonymous cookie-based identifier or an IP address; however, it would be much harder to identify a specific person. Although it may be theoretically possible, our systems are not designed to identify the specific user by name or email address. Therefore, our replies to Qs 9–13 are consistent with the fact that we treat both search cookie IDs and IP addresses as anonymous identifiers and have not designed our systems to correlate these anonymous identifiers with known individuals.

Question:

How long is Microsoft storing logged IP addresses?

Response:

Each business sets its own retention policy based on the need—which might range from less than 10 seconds to over 2 years. The purpose of retaining the IP address varies from service to service but generally is needed for quality of service monitoring and assurance.

Question:

How many requests from the PRC has Microsoft received for user IP addresses?

Response:

We have received several requests for information that did not meet our policy and legal requirements. We provided user addresses and IP information in only four cases, which were related to serious criminal investigations. We did not provide any of the contents of email communications,

Question:

How many requests for IP addresses has Microsoft complied with?

Response:

We have provided registration and IP information in four cases over the last two years. All four cases involved serious crimes: one involved an American student reported missing in China; the second was a murder case; the third, a pornography case; and the fourth, a hacking case involving theft of trade secrets. We did not provide any of the contents of email communications.

Question:

Has the PRC made requests for search terms, and if so, has Microsoft complied with any of the requests?

Response:

No requests have been made.

Question:

Are users' search terms tied to their email accounts, if they have a MSN email account?

Response:

No. Users' search terms are not tied to an email address or Passport user ID.

Question:

Many U.S. companies have been quick to point out that they reached a "compromise" with Chinese authorities for providing search engine technology to Chinese users under the premise that "getting their nose under the tent" will help them to expand access to information in the future. What happens, however, if the Chinese government tries to exert more control over your companies in the future—conceivably after your companies are more heavily invested in China's economy? Will your companies adhere to these new restrictions in the interest of shareholder profits—or is there an ideological line in the sand that you will not cross for money?

Response:

Our interaction with the Chinese government is a continuing process. We cannot predict what new approaches they may take with respect to censorship and customer information, either in the form of new regulations or in the ways they interpret and apply those regulations. Of course there are things we will not agree to do and it may at some point become impossible for us to continue to provide certain services in China. We do not think it is helpful to outline where those "bottom lines" may be while a number of the issues are in such a dynamic state.

Question:

Many of my constituents have asked me what many companies in your industry are adhering to a "double standard" when it comes to cooperation with world governments. Google, for example, has resisted efforts by the U.S. Justice Department to obtain certain information associated with user searches for pornographic material on the internet—this at the same time that the company was actively searching for a way to accommodate demands for content control from the PRC government as a condition of providing service to Chinese internet users. Why is it that it's ok to fight the demands of the U.S. government on principle when it comes to government compliance, yet it is perfectly acceptable to comply with the demands of the Chinese government? Is the libertarian ethic of internet companies selective based on revenue projections?

Response:

We defer to Google to respond directly to your concern about a double standard. We determined that we could comply with the DOJ subpoena in full compliance with ECPA without compromising our customers' privacy, because the subpoena asked only for aggregated search terms, not identifiable queries. However, the reality is not one of a double standard, but rather of numerous different standards from country to country—both as to the substance of regulations and the processes for applying them. Efforts to negotiate common international standards in these matters are only just beginning and are unlikely to produce uniform principles in the near future. Therefore, all Internet companies not only face different standards from place to place, but evolving standards in almost every country. That is the challenge of operating these services on a global basis.

[NOTE: Written questions for the record were submitted to Mr. Michael Callahan, Senior Vice President and General Counsel, Yahoo! Inc., but as of press time, responses had not been received by the Subcommittee on Africa, Global Human Rights and International Operations.]

[NOTE: Written questions for the record were submitted to the U.S. Department of State but, as of press time, responses had not been received by the Subcommittee on Africa, Global Human Rights and International Operations.]