AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

GOOGLE AND INTERNET CONTROL IN CHINA: A NEXUS BETWEEN HUMAN RIGHTS AND TRADE?

HEARING

BEFORE THE

CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

MARCH 24, 2010

Printed for the use of the Congressional-Executive Commission on China

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

U.S. GOVERNMENT PRINTING OFFICE

56–161 PDF WASHINGTON : 2010

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

CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

LEGISLATIVE BRANCH COMMISSIONERS

Senate

BYRON DORGAN, North Dakota, *Chairman*
MAX BAUCUS, Montana
CARL LEVIN, Michigan
DIANNE FEINSTEIN, California
SHERROD BROWN, Ohio
SAM BROWNBACK, Kansas
BOB CORKER, Tennessee
JOHN BARRASSO, Wyoming
GEORGE LeMIEUX, Florida

House

SANDER LEVIN, Michigan, *Cochairman*
MARCY KAPTUR, Ohio
MICHAEL M. HONDA, California
TIMOTHY J. WALZ, Minnesota
DAVID WU, Oregon
CHRISTOPHER H. SMITH, New Jersey
EDWARD R. ROYCE, California
DONALD A. MANZULLO, Illinois
JOSEPH R. PITTS, Pennsylvania

EXECUTIVE BRANCH COMMISSIONERS

Department of State, To Be Appointed
Department of Labor, To Be Appointed
Department of Commerce, To Be Appointed
At-Large, To Be Appointed
At-Large, To Be Appointed

CHARLOTTE OLDHAM-MOORE, *Staff Director*
DOUGLAS GROB, *Cochairman's Senior Staff Member*

CONTENTS

	Page
Opening statement of Hon. Byron L. Dorgan, a U.S. Senator from North Dakota; Chairman, Congressional-Executive Commission on China	1
Smith, Hon. Christopher H., a U.S. Representative from New Jersey; Ranking Member, Congressional-Executive Commission on China	3
Wu, Hon. David, a U.S. Representative from Oregon; Member, Congressional-Executive Commission on China	5
LeMieux, Hon. George, a U.S. Senator from Florida; Member, Congressional-Executive Commission on China	6
Davidson, Alan, Director of U.S. Public Policy, Americas, Google, Inc.	7
Jones, Christine, Executive Vice President, General Counsel, and Corporate Secretary, The Go Daddy Group	9
Hom, Sharon, Executive Director, Human Rights in China	11
Black, Edward, President and CEO, Computer & Communications Industry Association	15
Palmer, Hon. Mark, former U.S. Ambassador to Hungary	17

APPENDIX

Davidson, Alan	34
Jones, Christine	37
Hom, Sharon	41
Black, Edward	45
Palmer, Hon. Mark	49
Dorgan, Hon. Byron	52
Levin, Hon. Sander	53
Smith, Hon. Christopher H.	54

SUBMISSIONS FOR THE RECORD

Select List of Political Prisoners Punished for Online Activity, March 24, 2010, submitted by Senator Byron Dorgan	56
Statement by Chinese Internet Bureau of the Information Office of the State Council	67
Written statement submitted by Rebecca MacKinnon, Visiting Fellow, Center for Information Technology Policy, Princeton University	68
Questions and Answers submitted for the record	76

GOOGLE AND INTERNET CONTROL IN CHINA: A NEXUS BETWEEN HUMAN RIGHTS AND TRADE?

WEDNESDAY, MARCH 24, 2010

CONGRESSIONAL-EXECUTIVE
COMMISSION ON CHINA,
Washington, DC.

The hearing was convened, pursuant to notice, at 2:06 p.m., in room 628, Dirksen Senate Office Building, Hon. Byron L. Dorgan, Chairman, presiding.

Also present: Senator George LeMieux; Representatives Christopher H. Smith; David Wu; and Michael Honda.

OPENING STATEMENT OF HON. BYRON L. DORGAN, A U.S. SENATOR FROM NORTH DAKOTA; CHAIRMAN, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

Chairman DORGAN. The purpose of today's hearing is to examine China's censorship of the Internet and the challenge it poses both to advocates of free expression and to U.S. companies doing business in China. The recent controversy over Google's operations makes clear that the Chinese Government's regulation of the Internet is both a human rights and trade issue.

In the spring of 2000, Congress debated whether to support PNTR [permanent normal trade relations] for China. Supporters argued that opening China's markets would improve human rights and level the playing field for U.S. companies. The Internet was expected to lead the way, and it has brought some important changes. Today, China has 400 million Internet users, the most in the world. The Chinese Government, to its credit, has invested heavily in Internet infrastructure and sought to bridge the digital divide between rich and poor.

Yet, the larger hopes for genuine openness and freedom have gone unrealized. China's Internet users remain subject to the arbitrary dictates of state censorship. More than a dozen agencies are involved in implementing a host of laws, regulations, and other tools to try to keep information and ideas from the Chinese people.

The government also continues to strengthen controls over the Internet and to harshly punish citizens such as Liu Xiaobo, who use the Internet to advocate for human rights and political reform. I have a list here of political prisoners in China punished in recent years for Internet activities. It was drawn from the Commission's publicly accessible Political Prisoner Database. I request that this list be included in the hearing record.

As this list vividly shows, China's censorship practices and control of the Internet have had a terrible impact on human rights advocates. These include ordinary people who promote political freedoms or try to organize on line, or ethnic groups such as Uyghurs and Tibetans attempting to share information about ongoing government repression.

We also are learning that Internet censorship and regulation in China have serious economic implications for many U.S. companies, such as Go Daddy. China's Internet regulations often run against basic international trade principles of nondiscrimination and maintaining a level playing field.

Testifying before the Commission today is a representative from Google, perhaps the most potent Internet company in the world. In mid-December, Google was a victim of a highly sophisticated and targeted attack on its corporate infrastructure originating from China. Google announced this week that it will stop censoring its Chinese search engine, by rerouting its China searches to its Hong Kong site. The company also said it would also monitor and publicize any attempts at censorship of its Hong Kong site by the Chinese Government.

Google's decision is a strong step in favor of freedom of expression and information. It is also a powerful indictment of the Chinese Government's insistence on censorship of the Internet.

The Commission is dedicated to understanding the connections between trade and human rights in China. For that reason, we have called on five prominent American business leaders and human rights experts to discuss the impact of Internet censorship in China today. I look forward to hearing from the witnesses about possible ways for the U.S. Government, policymakers and businesses to respond to China's regulation of the Internet from both human rights and trade perspectives.

I wanted to say at the start of this hearing that we asked the Chinese Embassy if they would like to send a representative to appear before us today. They declined, as they always have. They did, however, send a statement. I want to move now to have that statement included in the hearing record. It is the first time that they have done so, and I want to include that in the record. Without objection, we will do so.

Chairman DORGAN. Yes?

Representative WU. Can we read a short section of it?

Chairman DORGAN. It's in your packet. I think we'll just include it in the record. In fact, there will be much of the statement with which we will disagree, but I do want it to be, nonetheless, a part of the formal hearing record. I also want to include, as a part of the formal hearing record, the prisoner list that is in your packet today and a submission of a testimony for the record by Rebecca MacKinnon, Visiting Fellow of the Center for Information Technology Policy at Princeton University.

So without objection, I will include all of those.

If we have comments—brief comments, opening comments—by others on the panel, I'd be happy to recognize them.

Representative SMITH. Mr. Chairman?

Chairman DORGAN. Yes, sir.

[The prepared statement of Chairman Dorgan appears in the appendix.]

[The letter from the Chinese Internet Bureau of the Information Office of the State Council appears in the appendix.]

[The prisoner list appears in the appendix.]

[The prepared statement of Rebecca MacKinnon appears in the appendix.]

STATEMENT OF HON. CHRISTOPHER H. SMITH, A U.S. REPRESENTATIVE FROM NEW JERSEY; RANKING MEMBER, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

Representative SMITH. Thank you, Mr. Chairman. As Ranking Member of the Commission, I applaud you for holding this very important hearing on Internet freedom.

As we know, Reporters Without Borders documents that in China alone at least 72 people are known to be imprisoned for Internet postings. The victims of the Chinese Government's assault on Internet freedom include the entire Chinese people, denied their right to freedom of expression, denied access to information, and often self-censoring out of fear.

Even beyond this, the Chinese Government's victims include other peoples, tyrannized by governments with which the Chinese Government sells or gives its advice on technologies and techniques of Internet repression. Reportedly, these include Cuba, Vietnam, Burma, Belarus, and Sri Lanka.

Yet we have seen some positive developments. We have seen that some U.S. IT companies really want to do the right thing. Yahoo! has established much stricter policies governing its interactions with repressive governments, especially with Vietnam. Yesterday, we had a hearing—and I chaired it—in the Tom Lantos Human Rights Commission on human rights in Vietnam. They have put personally identifiable information out of the hands of Vietnam.

Even while we were meeting, a member of the Human Rights Watch organization got an e-mail that Dr. Phan Hong Son, and I met with his wife when I was in Vietnam, obviously another country but borrowing from China, that he had just had his house invaded after spending four years in prison for posting on the Internet "What is Democracy," translated and downloaded from U.S. Embassy Hanoi. For that so-called crime, he got a jail sentence. Yesterday they raided his home. But Yahoo! has learned from that and put that personally identifiable information outside the reach of the secret police.

Google's transformation has been perhaps the most impressive over these last couple of years. In 2006, I chaired the first hearing on Internet freedom called "The Internet in China: A Tool for Freedom or Suppression?" The hearing responded to Yahoo!'s cooperation with Chinese Internet police tracking down the journalist Shi Tao, who is still serving a 10-year prison term for disclosing "state secrets," that is, e-mailing to the United States the Chinese Government's orders on what not to say on the 15th anniversary of Tiananmen Square.

Google, Yahoo!, Microsoft, among others, Cisco as well, testified at the hearing, which broke new ground on the issue of Internet freedom. Since 2006, we have had meetings with Google executives.

They have taken actions on their own accord, realizing, I believe, that the view that somehow the Internet would transform and open up China; when the Chinese secret police, the government, and the censors took over, it was doing precisely the opposite.

Two days ago, Google fulfilled its January commitment to stop censoring results on its Chinese search engine. This is a remarkable, historic, and welcomed action, and an important boost of encouragement for millions of Chinese human rights activists. Mark Palmer will testify in a few moments and will tell us how some 11,000 of the most influential people in China have signed onto Charter 08, not unlike Charter 77 in the Czech Republic, or Block 8406. It is a statement of human rights principles.

Well, every one of those people, every one—and I believe by extension the Chinese public—are greatly heartened by what Google has done. Despite the fact that they have gotten push-back from some, especially Microsoft—and we went into this last week at a hearing—they need to get with the program and join with the side of human rights rather than enable tyranny, which regrettably they're doing now.

Today, Go Daddy, the world's largest domain registrar, announced in its submitted testimony that it has decided to discontinue new .CN domain names at this time out of concern for the security of the individuals affected by the Chinese Government's new requirement for domain registration.

Go Daddy is the first company to publicly follow Google's example in responding to the Chinese Government's censorship of the Internet by partially retreating from the Chinese market. Google fired a shot heard around the world, and now a second American company has answered the call to defend the rights of the Chinese people. Go Daddy deserves to be praised for this decision. It is a powerful sign that American IT companies want to do the right thing in repressive countries.

Go Daddy and Google deserve more than praise for doing the right thing in China, they deserve our government's support—not lip service, but tangible, meaningful support. We want to see American IT companies doing the right thing, but we do not want to see them necessarily forced to leave China for doing so. That is why I have introduced the Global Online Freedom Act, a bipartisan bill that would seek to protect nonviolent political speech and nonviolent religious speech.

It will do so by requiring those IT companies doing business in China to disclose what it is that they're censoring. It will ensure that Radio Free Asia, Voice of America, and other American broadcasts are not censored. I, Mr. Chairman, was actually at an Internet cafe right before the Beijing Olympics and tried to access in that cafe one prohibited word after another, like the Dalai Lama, the Uyghurs, Wei Jingsheng.

I even tried to find out what they were saying about Manfred Nowak, the Special Rapporteur for Torture for the United Nations. What did I get? When I went to Manfred Nowak, I got what he said about Gitmo, not what he said about China, which was a scathing UN-backed report about the pervasive use of torture in the People's Republic of China.

This legislation would also hold to account those who have—once they've been designated as an Internet-restricting country—the companies would have to put personally identifying information out of reach of the secret police, thus protecting the dissidents and the religious believers and others who want to build a new China that is free and unfettered from the tyranny that currently exists.

So I would hope members of this distinguished panel might touch on the issue of the Global Online Freedom Act, but also obviously on China, which is why you are here. We thank you so much for taking the time to give us the benefit of your wisdom.

Chairman DORGAN. Are there others who wish to make statements? Congressman Wu.

STATEMENT OF HON. DAVID WU, A U.S. REPRESENTATIVE FROM OREGON; MEMBER, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

Representative WU. Thank you very much, Senator. I normally forego the opportunity to speak, but I think that this is truly a singular moment.

Let me make it clear that I'm not here to criticize any company, I'm here to praise Google in its singular action, its unique action in favor of Internet freedom and the tremendous example that it sets for others. It is heartening to hear that Go Daddy has decided to be number two. Two points define a line, three points define a plane, and pretty soon you have a cascade going.

Of course, I agree with the Chinese Government that every Chinese person and entity ought to obey the laws of the jurisdiction. It is clear to me that Google is in full compliance with Chinese law as far as its counsel can determine, and there is a difference between compliance and complicity. One can comply, and at great cost and risk, do so in a manner which is consistent with the values of the Internet and of Silicon Valley culture.

I think that what we need to do is to encourage the better angels of our nature, whether it is in corporate culture or in Chinese culture. One of the reasons why I think it's important for me personally to come here is to demonstrate that there is no historic or cultural incapability and no genetic incapability in advocating for and living a life of democracy for any particular culture or people.

So I want to salute Google's contribution to this ongoing debate. I want to encourage those in China, because it is a large, complex society, those in China who are in favor of both the rule of law and the enlargement of the sphere of civic freedom.

I want to encourage everyone in the Internet culture, which I believe is a very open culture that believes in the competition of information and ideas, to express themselves so more and more organizations, businesses will follow Google's example.

Of course, every company is different and will come to their own conclusions, but I think that on the divide between compliance and complicity, history will judge and one should be careful to be on the right side of history.

STATEMENT OF HON. GEORGE LeMIEUX, A U.S. SENATOR FROM FLORIDA; MEMBER, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

Senator LEMIEUX. Mr. Chairman, thank you for hosting this bicameral, bipartisan Commission meeting today. It's the first one I've had the opportunity to attend as a new Senator. But I want to add my voice in thanking Google for the great work that it is doing. I want to applaud them, as well as Go Daddy that we heard about today.

I want to just say to the Government of China, the message has to be that with great power comes great responsibility. They have a responsibility to allow their people to live freely and to have the information they need. We know that information, free information, is the beginning of the end of repression. It's the beginning of the end of tyranny.

So it is our responsibility, representing the government of this country, to insist upon that, whether it's in Venezuela, where yesterday a former opposition leader who ran for president was arrested, and the last television network in Venezuela is afraid of being shut down.

Whether it's in Cuba, where there is no free speech, where today the Ladies in White are protesting the arrest of political prisoners and the death of Zapata, who died. His mother is being arrested for protesting the death of her son. Whether it's in China, where political prisoners are being taken for the simple alleged sin of posting on the Internet and the chance to bring new ideas to this huge and important country in the world.

With great power comes great responsibility. So, I thank you, Mr. Chairman, for calling and chairing this hearing today, and look forward to the testimony of the witnesses.

Chairman DORGAN. Senator LeMieux, thank you very much.

Anybody else want to make a statement, a very brief statement? [No response.]

All right. Let me begin with Alan Davidson, Director of U.S. Public Policy with Google. He is the head of U.S. Public Policy. Prior to joining Google, he was Associate Director of the Center for Democracy and Technology. He is also an Adjunct Professor at Georgetown University's program in Communications, Culture, and Technology. He is trained as a computer scientist. He holds degrees in mathematics and computer science from MIT, and a J.D. degree from Yale Law School.

Mr. Davidson, let me join others on this panel who have complimented Google for its decision, a difficult but nonetheless a courageous decision, one that I think is absolutely correct. Thank you for being here. You may proceed.

I would say to all of the witnesses, that your entire statement will be made a part of the permanent record and you may summarize.

STATEMENT OF ALAN DAVIDSON, DIRECTOR OF U.S. PUBLIC POLICY, AMERICAS, GOOGLE, INC.

Mr. DAVIDSON. Well, thank you, Mr. Chairman. Chairman Dorgan, Cochairman Levin, members of the Commission, thank you for inviting Google here today, and thank you for your commitment to

a free and open Internet. I would also say, particularly, thank you for your very supportive comments just now. They are very meaningful to our company at this time.

Last summer, a young woman was shot on the streets of Tehran during protests over the Iranian elections. No film crew witnessed her death, no reporter was there to cover her story, but a bystander with a cell phone captured it on video. That video was posted on YouTube and it was watched by literally tens of millions of people around the world.

Despite the government crackdown on communications, Neda Agha-Soltan's tragic death became a galvanizing force for international outrage. This is the essence of expression online: unexpected, unpredictable, but capable of capturing the minds and the hearts of millions of people around the world. It is for this reason that the growing restrictions on speech online demand a commitment from companies, civil society, and governments together to protect Internet freedom.

I would like to make three points today. First, Internet censorship is a global threat to human rights and economic opportunity. The growing problem with Internet censorship is not isolated to one country or one region. As Secretary Clinton recently expressed, the impact on human rights and the global marketplace is profound.

At Google, we have experienced this first-hand. In the last few years, more than 25 different governments have blocked Google services, including YouTube and Blogger. For example, YouTube has been blocked in Turkey for over two years because of videos that allegedly insult Turkishness. In 2009, during the elections in Pakistan, the government ordered service providers there to block opposition videos on YouTube.be.

Then there was our experience in China, where the last year has witnessed a measurable increase in censorship in every medium, including the Internet. That leads me to my second point, which is that the situation in China has led Google to implement a new approach there.

In mid-December, we detected a highly sophisticated attack on our corporate infrastructure originating from within China. While Google is frequently a target of attacks, it soon became clear that this was not a routine security incident. We discovered that at least 20 companies from a range of industries had been similarly targeted. The attack was unusually sophisticated, with a principal but unsuccessful goal of accessing G-mail accounts.

In our investigation, we discovered that entirely separate from these attacks, the accounts of dozens of G-mail users who were advocates for human rights in China had been compromised through malware and phishing attacks—again, totally separate, but very disturbing.

These circumstances, as well as the increasing attempts over the past year to limit speech online, led us to announce in January that we no longer felt comfortable censoring our search results in China. So earlier this week we stopping censoring our search services on Google.CN, our search site in China. Users visiting Google.CN are now being redirected to Google's site in Hong Kong,

where we are offering uncensored search in simplified Chinese designed specifically for users in China.

Figuring out how to make good on our promise to stop censoring search on Google.CN has been difficult. We believe this new approach is a sensible solution to the challenges that we face. We very much hope that the Chinese Government respects our decision, although we are well aware that at any time its great firewall could prevent users from accessing our services. Indeed, we have already seen intermittent censorship of certain search queries on our Hong Kong site.

My third point is that government should do more to protect Internet freedom around the world. Internet, government, and nonprofit groups have a shared responsibility to protect a free and open Internet. We strongly support the Global Network Initiative [GNI], which is a unique collaboration of human rights groups, investors, and companies to create standards for engagement that protect privacy and free expression.

More corporate members are needed to reach the Global Network Initiative's full potential, but no single company and no single industry can tackle Internet censorship on its own. Government action is needed. Specifically, we believe that Internet freedom must become a major plank of our foreign policy. The free flow of information should be an important goal of diplomacy, of foreign assistance, and our engagement on human rights.

Internet censorship should also be a key part of our trade agenda, as we lay out in some further detail in our testimony. Governments around the world should themselves be transparent when they make demands to censor or when they request information about users. Finally, Google also supports efforts of Congress and the Administration to fund technical solutions to counter censorship.

In conclusion, I want to thank you for your continued leadership in the fight against censorship online. We look forward to working with you to maximize access to ideas and to promote Internet freedom around the world.

Thank you.

Chairman DORGAN. Mr. Davidson, thank you very much. We appreciate your testimony.

Next, we will hear from Christine Jones, Executive Vice President, General Counsel, and Corporate Secretary of the Go Daddy Group. She is responsible for all legal affairs of the Go Daddy Group, as well as domain services, network abuse, government relations compliance, and legal departments.

She previously was an attorney specializing in private commercial litigation, and before that worked for the Los Angeles District Attorney's Office. In addition to being a lawyer, Ms. Jones is a CPA with degrees from Auburn University and Woodyear Law School.

Ms. Jones, welcome.

[The prepared statement of Mr. Davidson appears in the appendix.]

STATEMENT OF CHRISTINE JONES, EXECUTIVE VICE PRESIDENT, GENERAL COUNSEL, AND CORPORATE SECRETARY, THE GO DADDY GROUP

Ms. JONES. Thank you, Mr. Chairman and members of the Commission.

For a few years now we have noticed that from time to time it is not possible to access Go Daddy.com in China. We are not sure why. One could infer it is because we register and host human rights and other Web sites that are deemed improper by Chinese officials, but we have never actually been told the reason.

Regardless, every time it happens, millions of Chinese nationals who try to visit our Web site, or the Web sites of our customers, are disappointed to find that Chinese censorship has kept them from free access to the Internet sites of their choice.

This is frustrating, as you might imagine. But I am not going to dwell on that. Instead, I want to briefly touch on five issues that are explained in more detail in my written testimony, specifically: monitoring and surveillance of Internet activities in China; DDoS [distributed denial of service] attacks originating in China; spam; payment fraud; and then finally what we feel the U.S. Government can do to help alleviate some of these issues. Then, of course, I would be happy to answer any questions you may have.

So, first, China's examination of Internet activities of its citizens has increased in recent months, and I mean very recently. Let me give you an example. This, Congressman Smith, plays into what you talked about in your opening statement.

We have been offering the .CN domain name extension for about six years. So, for instance, chairmandorgan.CN, that type of thing. In the beginning, the .CN authority, which is called CNNIC [China Internet Network Information Centre], required us to collect the first and last names of the registrant, a physical address, a telephone number, and an e-mail address. That was it. That is very typical of what is normally required by that type of domain name extension.

In December of last year, CNNIC announced that we'd have to start collecting a photo ID, in color, from the head to the shoulders, a business ID, and a physically signed registration paper for all new .CN registrations.

In February, two months later, CNNIC announced that we had to provide the increased documentation for all current .CN registrations. So, in other words, we were going to have to retroactively apply those rules, and if we failed to provide it, the domain names were going to stop working. Now, keep in mind, some of these names had pointed to fully functioning Web sites for as long as six years.

We were immediately concerned, of course, about the motives behind the increased level of registration verification required by CNNIC. It didn't make sense to us that the identification procedures that had been sufficient and in place since 2005 were apparently no longer sufficient from China's standpoint, and no convincing rationale for the increase in documentation was ever provided to us.

We were also concerned by the sort of ex post facto or retroactive nature of the new requirement. In other words, at the time the affected Chinese nationals registered their domain names they

weren't required to provide the photo ID or the business identification and the other identification now being required by CNNIC.

Because the new documentation requirement was to be retroactively applied to registrants who had previously registered their Web site, as I said in some cases years before, it appeared to us the intent of the new procedures was based on a desire by the Chinese authorities to exercise increased control over the subject matter of domain names registered by Chinese nationals.

Now, Go Daddy has been registering domain names since 2000. We serve as an accredited registrant for dozens of domain name extensions. We have 40 million domain names under management, by far the most of any company in the history of the Internet. We've done this a lot. This is the first time any registry has ever asked us to retroactively obtain information on individuals who registered a domain name through our company, the first time.

We are concerned for the security of the individuals affected by CNNIC's new requirement. Not only that, but we are concerned about the chilling effect we believe the requirements could have on new domain name registrations, and therefore the free exchange of ideas on the Internet.

For these reasons, as you mentioned, Congressman, we have decided to discontinue offering .CN domain names at this time. We will, however, continue to manage the .CN domain names of our existing customers, those people whose identifications are now in the process of being revealed to the Chinese officials.

Second, I want to touch on DDoS attacks that was briefly mentioned by my colleague from Google. In the first three months of this year, we have repelled dozens of extremely serious attacks on the systems that host our customers' Web sites, attacks that apparently originated in China.

Of course, that number only includes the attacks that we had to get involved in. That does not include the attacks where our systems automatically averted the attack. The recent cyber attacks on Go Daddy and Google and other U.S. companies are troubling, but they are not new. They reflect a situation that Go Daddy has been combating for many years.

Third, on the spam issue, we found that an overwhelming majority of Web sites promoted through spam are hosted in China, often at service providers that choose to completely ignore complaints of spam and other types of illegal activity. We see no assistance from Chinese officials to combat this problem. In fact, it seems to be just the opposite. The force of the Chinese Government appears to be being used to justify the activities of those who engage in spam as a business model as opposed to helping to stop it.

Fourth, on payment fraud, there is significant payment fraud originating in China. The payment fraud trends associated with China-based users include the widespread use of compromised U.S. and U.K. credit cards, for example, as well as gift cards, other online payment forms like Allipay, which would be the Chinese version of PayPal. Substantial payment fraud originating in China. Again, no action by Chinese officials to help us combat that problem.

Fifth and finally, we want to talk about what we think the U.S. Government can do to help us. Our primary mission at Go Daddy,

of course, is to promote secure, easy, equal access to the Internet to people around the world and we wholeheartedly agree with Google on that principle. We are also committed to ending the improper use of the Internet, including for the invasion of personal privacy or to limit freedom of expression. It is a big problem.

We hope the U.S. Government will use its influence with authorities in China to increase Chinese enforcement activities relating to Internet abuse while encouraging the free exchange of ideas, information, and trade. This would include the retraction of China's recent policies relating to the registration of .CN domain names.

We were encouraged to see there is a briefing this afternoon to discuss the mission of the new Senate Global Internet Freedom Caucus, which we hope will seek to promote online freedom in China and other countries. We are also following closely Congressman Smith's online freedom legislation which purports to put the U.S. Government on the side of U.S. companies and human rights activists when they deal with repressive governments, so we applaud you for that.

Of course, we are sincerely grateful for this Commission's attention to these important issues. We understand there is no silver bullet, but we are proud to at least be part of the process.

Thank you.

Chairman DORGAN. Ms. Jones, thank you very much.

Next, we'll hear from Sharon Hom. Sharon is the Executive Director of Human Rights in China and Professor of Law, emeritus, City University of New York School of Law. She has testified on a variety of human rights issues before the U.S. Congress and the E.U. Government body. She has led Human Rights in China, an organization, in its consultations with companies doing business and investing in China. In 2007, the Wall Street Journal named her as "One of the 50 Women to Watch for Their Impact on Business."

Ms. Hom, welcome. You may proceed.

[The prepared statement of Ms. Jones appears in the appendix.]

STATEMENT OF SHARON HOM, EXECUTIVE DIRECTOR, HUMAN RIGHTS IN CHINA

Ms. HOM. Thank you, Mr. Chairman. I want to thank the members of the Commission for your solidarity, your leadership, and your support for the very difficult struggle and challenges to promote freedom of expression in China.

I would like to request that my written statement be entered into the record and I would like to use my oral time to briefly comment on some of the Chinese official responses to Google's actions. I will then focus on the case of Liu Xiaobo, and conclude with some recommendations for discussion. I welcome your questions.

As the comprehensive and excellent CECC 2009 Annual Report, the State Department China Country Report, and recent UN human rights reviews of China demonstrate, the human rights violations in China are serious, systematic, and widespread.

In addition to the economic, political, and increasingly soft power leverage of China, China is exerting enormous control over expression on the Internet through state-of-the-art technology, its state secrets and state security system, the police and security apparatus, and resulting self-censorship. All of this has been extensively

mapped and inventoried in these reports. Rebecca MacKinnon's submitted testimony provides a very good map-out of the technology.

The Chinese responses on Google's decision are obviously a complex story still in progress, as attested to by the headlines this morning. After an initial effort to accuse Google of being a CIA operative—that didn't last very long—the official Chinese responses reflect a combination of: an effort to rhetorically repackage the Google decision; stating the obvious and asserting that the Chinese authorities are acting in accordance with law; and finally, making some ludicrous statements, such as there is no censorship in China, and that the Internet is fully open, et cetera, and claiming this development of events has no impact on China's international image or on U.S.-China relations. Clearly, Google, as a major economic player, is very important and has an impact not only on the Internet, which is global, but also on innovation and creativity in development of the IT sector in China, with implications for the region.

So what is at issue here, in addition to the role of the marketplace of ideas, is whether China is really ready and willing to be a mature, responsible member of the international community, one that respects its international obligations, including human rights obligations, as well as under the WTO and other trade obligations.

Despite the official mantra that any foreign company doing business in China has to comply with local Chinese law—which is quite complex—the Chinese answers to date to the key question of whether Google's actions are in fact in compliance with Chinese law are vague and unclear. Ironically, Google's decision does comply with certain aspects of Chinese law, particularly constitutional provisions that protect human rights, freedom of expression, and privacy rights. So, I think it is important to ask, what Chinese law are we talking about when we say that companies have to comply with Chinese law? Regarding the cross-border impacts that have already been referred to by Representative Smith, the experience of Human Rights in China's [HRIC] own staff illustrates that the Chinese authorities' repressive tactics at home, both low-tech and high-tech, extend to Chinese nationals and human rights defenders abroad. Such tactics include blacklisting, surveillance, and even inhumane denials of permission to return to China for family funerals. This is not part of a "harmonious society" and does not reflect Chinese cultural values.

Additionally, the Chinese authorities have been very active, and increasingly so, in preventing independent human rights groups from successfully applying for UN accreditation. We welcome the U.S. Government's renewed commitment to engage with the human rights system at the United Nations.

My written testimony outlines some of the ways in which HRIC is focusing on supporting Chinese lawyers, activists, journalists, writers, and other rights defenders, specifically through our technology initiatives, including the distribution of over 200,000 electronic biweekly newsletters into China, in which HRIC publishes Chinese writers and censored news and discussion. We have also built an HRIC YouTube channel and use social networking tools like Twitter—all accessible from inside China. Even though YouTube is blocked, an estimated 26,000 to 30,000 people still

reach YouTube, and some of the protest videos that are posted on our YouTube station have gotten hundreds of hits.

Let me move quickly to the case of Liu Xiaobo, who really exemplifies the challenges facing the front line in the struggle for freedom of expression. We welcome the CECC list featuring individuals who, because of their Internet activities, are paying a very heavy price.

Liu Xiaobo is a prominent independent intellectual. He has been a long-time advocate of political reform and democracy and human rights, and he has been an outspoken critic of the Chinese Communist regime and one of the key drafters and organizers of Charter 08.

Under the full glare of international attention, with international diplomatic representatives outside the courtroom, on Christmas day, a court in Beijing convicted Liu Xiaobo of inciting subversion of state power and sentenced him to 11 years in prison and 2 years deprivation of political rights. What was this for? It was for six essays that he had published online between 2005 and 2007, in addition to his key Charter 08 role.

HRIC's bilingual quarterly publication, the China Rights Forum—copies are available today for Members of the Commission—translated these six articles and all of the legal documents of Liu Xiaobo's case. We asked the question, so what does constitute inciting subversion of state power in China?

In his article "The Many Aspects of CPC Dictatorship," Liu Xiaobo describes the post-Mao regime and argues that, unlike the era of Maoist totalitarianism, this regime is more skillful in using pragmatic, flexible control to maintain stability. But it is a loyalty that is bought by the promise of a comfortable life that has a soul that is rotten to the core.

His article "Can It Be That the Chinese People Deserve Only Party-Led Democracy," not only presents a critique of the party, but actually raises a challenge to the Chinese people ourselves: Liu powerfully reminds the readers that no totalitarian, authoritarian state stayed in power because of the power of the ruler, but rather, because the people knelt down.

Finally, the articles, "Changing the Regime By Changing Society: The Negative Effects of the Rise of Dictatorship," and "Further Questions," Liu's article about child slavery, expose the extreme government corruption and the lack of accountability that continues to persist for thousands of children who are kidnapped and used as slaves.

The verdict sentencing Liu Xiaobo actually cites the number of online clicks registered for each article, ranging from 57 to 5,000 clicks. Those do not necessarily translate into the number of individual readers. However, all of these articles were posted on Web sites that are censored in China. So that means Liu Xiaobo has been convicted to 11 years in prison for inciting subversion of state power based in part upon the "evidence" of between 57 to 5,000 clicks on Web sites that can't be accessed from inside China. This is a testament about the insecurity of those in power, but it is also a testament to the power and the necessity of freedom of expression.

I know my time is up, so let me quickly conclude with a few points for discussion.

First, on individual cases, the CECC Political Prisoner Database is extremely important and we would urge the Commission to link your advocacy work on behalf of these cases with decisions that have been reached by international independent expert bodies. Shi Tao, who is still in prison, in fact, received a decision from the UN Working Group on Arbitrary Detention back in 2006, determining that his detention is arbitrary and in violation of international human rights. We would urge that you press for his release based on this determination by a UN independent expert body. This is not interference in China's "internal" affairs or the Chinese legal system.

Second, we urge greater support for developing specific technologies, for example, expanding uncensored online platforms, developing more circumvention tools and safe dissemination methods, and promoting expanded use of social networking tools.

Finally, in terms of the companies, there needs to be more encouragement to companies to join multi-stakeholder initiatives. We especially appreciate the letter from Senator Durbin to 30 technology companies, urging them to join the Global Network Initiative, of which Human Rights in China was one of the founding participants.

The Google decision this week really illustrates the possibility of moving beyond an either/or mentality and of thinking that the choices are to stay and censor or to leave the country, because technically Google has not left the country. We do not know if this One Country, Two Systems move will actually work, but technically Google is still in China and Google has been able to act in a principled way. Whether this will work is uncertain, but as Sergei Brin has stated, "The story is not yet over and the future is a long time."

Chairman DORGAN. Ms. Hom, thank you very much for your testimony.

Next, we will hear from Mr. Edward Black, the President and CEO of Computer & Communications Industry Association. He has been President and CEO of that organization since 1995. He serves on, and previously chaired, the State Department's Advisory Committee on International Communications and Information Policy. He has also served in the Office of Secretary in both the Commerce Department and the State Department. He holds a B.A. from Muhlenberg College and a J.D. from American University, Washington College of Law.

Mr. Black, it is good to see you. Thank you. You may proceed.

[The prepared statement of Ms. Hom appears in the appendix.]

STATEMENT OF EDWARD BLACK, PRESIDENT AND CEO, COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

Mr. BLACK. Thank you, Mr. Chairman and members of the Commission. It is an honor to be here today to have a chance to testify on this very important subject of Internet freedom in China.

For too long the U.S. business community has had insufficient support from the U.S. Government in responding to other nations' efforts to censor or spy on their citizens and to interfere with the

reasonable flow of services, products, and information. Companies are on the front lines in the battle for Internet freedom, but when they are confronted with foreign government demands, the governments that represent these companies must lead in the defense of Internet freedom and free trade.

Our Nation founded the Internet. Our government should have been, and now needs to be, out there promoting multilateral international understanding in order to maximize freedom of the Internet.

Totalitarian regimes depend on controlling the flow of information, both domestically and from the outside world. The Internet is no exception, and it is a tempting target to turn into a tool of state control. We must protect Internet openness from those who want to use it for repression and for many seemingly noble, well-meaning efforts to control specific content or monitor Internet traffic that also may chip away at its openness.

My testimony today is designed to focus on human rights aspects of censorship, on the trade aspects, and the underlying principle of Internet freedom.

The Internet can be the greatest tool in history for people to gather information, communicate, and do many other things that the human race has tried hard to improve on over the years, or the Internet can be among the greatest tools for political repression, depending on how it is used. If we fail to take actions, others may pervert the Internet and finally bring about the Orwellian future we thought we had avoided, one in which governments perpetually spy, surveil, censor, and control, and say they are doing it for our own good.

The U.S. Government must consistently treat Internet freedom as a priority human rights issue in its dealings and communications with foreign governments. We are here today partly because of the high-profile battle of Google in China, but the number of companies and countries impacted are far greater.

There are few easy answers for companies as they try to bring their technology services and communication tools into nations that have different rules about free speech and freedom of expression. Without the backing of their own government, companies often are faced with the unappealing decision to follow local laws or else exit the market. Staying and engaging can in some cases offer appealing choices to citizens in a repressive country, so the choices are not always simple or easy.

As a trade issue, censorship has been ignored. The United States is an information economy. U.S. companies are leading vendors of information products and services. Filtering American content and services has the effect of filtering American competition, and combating it should also be on the top of our trade agenda.

Restrictions of Internet traffic affect trade in a number of ways. Such restrictions may constitute a non-tariff barrier, may be an unfair rule of origin, may be a violation of the Principle of National Treatment. The violation of the WTO's very strong rules on transparency and access and administrative review of regulations has had no impact in the world of Internet review and regulation.

There must be a trade remedy when a country blocks access to a U.S. Web site and the advertising on those sites is also being

blocked and the trade in the products and services advertised are interfered with. The European Union, by the way, should be praised at this point, because in 2008 they passed, overwhelmingly, a resolution recognizing Internet censorship as a trade barrier. The vote was 571 to 38. There needs to be further implementation of that resolution, but it was an important step in the right direction.

These are some steps that we think can be taken to promote Internet freedom. First of all, the U.S. Government should, on an ongoing basis, investigate cases when Internet censorship is brought to their attention. The U.S. Trade Representative [USTR], the State Department, and the Commerce Department all have responsibility to raise Internet restrictions in the dealings they have with countries on many issues around the world on an ongoing basis.

Our Nation has missed the opportunity to use existing trade agreements to constrain Internet restrictions, censorship, and surveillance. The USTR should be highlighting Internet censorship in its trade reports. In 2006, the USTR issued a report that was billed as a top-to-bottom review of U.S.-China trade relations. The report discussed simple infringement of intellectual property, which we don't support, yet did not mention Internet censorship policies.

The USTR has a very important annual Special 301 review process focused on identifying intellectual property problems around the world. I think we should replicate that process for Internet freedom and violation thereof.

The USTR should review foreign government restrictions on the Internet, taken in the name of censorship or otherwise, and seek ways to take appropriate action. We need to negotiate provisions that promote Internet commerce, openness, and freedom in our trade agreements and in other agreements. I will not go into the details on the need for supporting GNI, but it's a great initiative and we do actively support it.

I want to make another point. The Internet freedom begins at home as well. The United States must lead by example. We need to discourage censorship and surveillance ourselves. We need to restrict intrusive practices such as deep packet inspection and think twice before attempting to block content which we perceive as unsavory. Once openness erodes, it is very hard to get it back.

When we go abroad advocating these principles we cannot go with dirty hands. Our credibility is critical if we are to be an articulate advocate in the international community. If our government leads the fight for international freedom by example at home and negotiations around the world, it can support U.S. companies who are trying to ethically compete in challenging markets.

In conclusion, let me just say that China's policy of coerced censorship has now become a matter of global public concern. If the U.S. Government does not push Internet freedom to the top of our priority list now, foreign governments all over the globe will conclude that they are free to pick off individual companies and intimidate them into submission.

We need to elevate this issue to the top of our diplomatic and trade agenda. We must be consistent with our own Internet freedom policies and fight for Internet freedom as a common principle so other nations understand our commitment to curbing censorship

of the Internet and threats to Internet freedom in whatever form they manifest.

Thank you.

Chairman DORGAN. Mr. Black, thank you very much.

Finally, we will hear from Ambassador Mark Palmer. Ambassador Palmer served in the U.S. State Department from 1964 to 1990, and was formerly Deputy Assistant Secretary of State for the Soviet Union and Eastern Europe, and U.S. Ambassador to Hungary. He was instrumental in the establishment of the National Endowment for Democracy, and currently is president of Capital Development Company, LLC, and vice chairman of the Center for Communications, Health, and the Environment. He is a graduate of Yale and a widely cited author.

Mr. Ambassador, welcome.

[The prepared statement of Mr. Black appears in the appendix.]

STATEMENT OF MARK PALMER, FORMER U.S. AMBASSADOR TO HUNGARY

Ambassador PALMER. Thank you, Senator.

French diplomats actually try to speak last in the hope that they will be remembered best, so I'm glad to be speaking last.

My written testimony emphasizes in the outset my optimism about China. I think, having served and lived in Communist countries a good part of my life, that we often underestimate what is going on among elites, and we know what's going on among the publics, 400 million of whom are on the Internet. Even Hu Jintao brags that he's on the Internet. So I think it's a mistake for us to assume that this very strong reaction to the admirable actions of Google or Go Daddy now, that that's the end of the story. I think there's a lot going on in China that we should be optimistic about.

But I want to focus in my oral remarks today on a story. I want to tell a story. Some of the students who were present on Tiananmen Square during 1989 came to the United States and earned doctoral degrees in computer sciences from leading American universities. They realized the enormous popularity and the potential of the Internet in China and were urged by Chinese still in China to find ways to use their computer engineering skills to combat growing censorship and the overall decline in human rights.

Beginning in the year 2000, they have developed a system of software and servers which, over the past decade, has grown to be the world's largest circumvention system, providing for roughly 90 percent of anti-censorship traffic in China and worldwide.

About a million Chinese today and hundreds of thousands of Iranians are using this system. It works through the distribution of encrypted, secure, free software and by constantly switching IP addresses, up to 10,000 times per hour, on dedicated servers located across the world. They have built and staffed this system with volunteer labor and virtually no financial support from anyone else.

The major limitation on this Global Internet Freedom Consortium's [GIF] ability to serve even much larger numbers of users and to bring down the firewall altogether is simply money. They have had to make hard choices between serving a surge in Iranian

users last summer and fall and reducing their availability to Chinese users as their servers were crashing.

GIF needs to buy many more servers and finally to be able to support full-time staff. Competing with and staying ahead of over 50,000 heavily financed engineers and censors in China requires a dedicated and properly financed team. We spend, Mr. Chairman, $800 million a year on Voice of America, Radio Free Asia, and other old media and we spend $1.7 billion on U.S. AID's democracy programs. Surely we can, and should, spend $50 to $100 million a year on a system or systems to circumvent Internet censorship and bring down this firewall.

Realizing the enormous success of this Global Internet Freedom Consortium and its potential, a bipartisan group of your colleagues, Senators and Congressman, appropriated $15 million in 2008 to begin to scale up this system and any others which could demonstrate proven ability to circumvent Internet censorship in China, Iran, and elsewhere.

In 2010, as you know, another $30 million was appropriated. In my 26 years within the State Department and 20 years outside working on democracy and human rights, I have never been more convinced of the power of any innovation to help those still living in one of the world's 43 remaining dictatorships, half of them Chinese, with the ability to liberate themselves. And I also have never been more appalled—I repeat, appalled—at the State Department's refusal to do what is so clearly in the national interest of the United States.

In flagrant and now repeated violation of congressional legislation, my old home, the State Department, has refused to use the appropriated funds to scale up an existing successful circumvention system. State Department staff-level officials have made a mockery, first of Secretary Rice's, and now of Secretary Clinton's, frequently voiced and sincere commitments to help ensure freedom of the Internet.

Let us take just one dimension of American national interest. There is a profoundly false understanding of the Google-China issue, as if Google must lose its China market because it no longer accepts Google.CN censorship. If the United States acts in the manner that we seek and people in China can access Google.com, whether in Hong Kong or here, you should sell your Baidu stock short and watch Google pick up support from Iran, Syria, and elsewhere.

Google is in a fight, and a martyred defeat will not help the cause. It, too, should be pressing the State Department in working with GIF. If it does so, its franchise throughout the world will be enhanced by orders of magnitude for being not merely a wounded victim, but the provider of enhanced closed society access to the Internet.

Fortunately, five of your colleagues here in the Senate wrote to Secretary Clinton on January 20, Senators Brownback, Casey, Kaufman, Kyl, and Specter, and they, in the strongest possible terms, have said enough is enough to the State Department, that they have to begin to fund the existing circumvention systems.

Senator Brownback placed holds on four senior State Department appointments and is prepared and took it off when some peo-

ple in the Department indicated a willingness at least to talk. But he and Senator Kyl and others are willing to put the holds back on if, within a week or so, we don't get a serious indication that they're engaging and are going to respect the will of this Congress on this critical national issue.

Let me just conclude by urging this Commission, which does such wonderful work, that you join your colleagues in urging the State Department to do what we all agree with, which is to circumvent this censorship.

Thank you, Mr. Chairman.

[The prepared statement of Ambassador Palmer appears in the appendix.]

Chairman DORGAN. Ambassador Palmer, thank you very much. We will do just that. We appreciate your testimony and your appearance.

I am told that there are four votes that have just begun in the U.S. House. What I'd like to do, with the consent of my colleagues, is to recognize the three House Members for a series of lightening-round questions before they have to rush out of here. I do want to have them have the opportunity to ask questions of the witnesses.

Representative SMITH. Thank you very much, Mr. Chairman. I really appreciate it.

Ms. Hom, you mentioned the outrageousness of the Chinese Government saying that there was no censorship on the Internet. When Chi Haotian was here in town during the Clinton Administration and made the same statement: that no one died at Tiananmen Square. We put together a hearing, and like you, Mr. Chairman, invited the Chinese to testify. He was a no-show. We even had a People's Daily editor say how he saw and witnessed people dying.

Hopefully it's so laughable and so embarrassing to the Beijing leadership that such outrageous statements will cease. The Universal Periodic Review was last done on February 9, 2009, on China. It only takes, as you know, one-third—one-third—of the member states on the UN Human Rights Council to call for a hearing on any country.

The U.S. Government should call for that vis-a-vis China to look at this. It could be done. It would bring the great spotlight on what they're doing on the Internet and on other human rights abuses. Your thoughts on that. I have so many questions, but we don't have time, so I'll just leave it at the one.

Representative WU. Thank you, Mr. Chairman.

I just want to ask one question of the witnesses, and that is for each of you, whether it's Google or Go Daddy or the organizations that you represent, if you have one, two, or three things that we could do, that the Federal Government could do in an operational way to help you in each of your respective efforts, different efforts, I would be very interested in hearing your responses. I suspect, Ambassador, that I know what your top one will be, but I'll look forward to hearing it.

I just want to take one moment to say that I couldn't help but notice that four out of five witnesses are legally trained. There is a lot of criticism at times about the litigious nature of American society and the number of lawyers we have, and so on and so forth.

I just want to say that my response to that has been, in the international context, show me a society where there are more attorneys than generals, and that's probably going to be a democracy. Show me the reverse and the story is not so good. So, you know, everything has its price. Thank you, Mr. Chairman.

Chairman DORGAN. Congressman?

Representative HONDA. Thank you. I can think of a country that's been led by a teacher. They haven't had the need for a military since they started. So, on behalf of teachers, I think that we can learn. I guess my mother says it best: "You've got two eyes, two ears, one mouth. Use them accordingly."

My question would be Mr. Smith's question regarding the Universal Periodic Review asked to Mr. Edward Black and to Ambassador Mark Palmer. In closing, I would like to thank you for a nice, well-balanced presentation for us to be able to listen, learn, and act.

Thank you.

Representative SMITH. Mr. Chairman, just very briefly. The Chinese statement submitted for the record cites international norms that they feel that they ought to, and you, like Google and Go Daddy, ought to live up to. Your views on the Global Online Freedom Act. If you all could provide us with that I'd appreciate it. I am sorry we have to go.

Chairman DORGAN. Let me thank my colleagues from the House. They are active participants in this Commission and we're sorry they have to go to vote, but appreciate their being here.

Mr. Davidson, can you tell us a little about how this works with the Chinese coming to an American company saying, we need your cooperation in censoring certain things. What types of information have authorities asked be to censored? How do they instruct? How do they deliver the information of what they want censored? I mean, can you give us some organic notion of how this works?

Mr. DAVIDSON. Well, let me try and give a general notion, because in some ways actually we are not actually permitted to talk about all of the requests that we get that are given to our employees in China, or not even necessarily our employees.

Chairman DORGAN. Permitted by the Chinese, you mean?

Mr. DAVIDSON. Right. So I think I'd be happy to characterize it.

Chairman DORGAN. But are you permitted to do it outside of China? [Laughter.]

Mr. DAVIDSON. We actually don't share a lot of information outside of China about what's happening. It puts us—and I think that gets to the heart of it—in a terribly difficult position, which is that there's not very much transparency at all about what's being requested and whether it's being requested of everybody, whether there are special requests or not. That places us in a terribly difficult position. I would say, outside observers have been able to derive quite a bit about the kinds of requests that come.

I think you can see that they're far-ranging, political in nature, and quite different from the kinds of results that we've had at other hearings that have showed the differences in the results that one gets from a censored version of the large search engines, including ours, and the uncensored versions. So I think that's part of why we ultimately felt that we needed to make this change, be-

cause the lack of transparency particularly makes it extremely difficult.

Chairman DORGAN. Well, I admire the judgment, and I've indicated that to you. What I'm trying to understand is, when you go to China to do business is there someone in China that says, all right, you are here now, you are on Chinese soil, we do business the Chinese way, and here is a set of written instructions, and by the way, in order to do business here you will follow them to the letter. Is there something in writing someplace that describes to your company what your obligations are under what they perceive to be Chinese law?

Mr. DAVIDSON. We operate under a license in China and I think, in part, the problem that I think we all—the companies that operate there—are trying to address in things like the GNI is dealing with the fact that the requests can be brought and that they do not always appear to be operating through the rule of law. So it's not like getting a court order from a U.S. judge, so I think that part of the concern is that we would like there to be more transparency and a clearer process than there has been. I could leave it to others who have had this experience as well in China.

Chairman DORGAN. Ms. Jones, you indicated that there was substantially increased Chinese Government activities December of last year and February of this year. Was there any discussion by the Chinese authorities about why they were doing this? Was there, in fact, admission that they were increasing activities or did the Chinese say, all right, here are the new rules?

Ms. JONES. No. In fact, if I could briefly respond to your question earlier, we wish there was a rule book. We wish there was the book that you could set on the table and say, here's what you have to do. But to your knowledge, that doesn't exist.

We just, from time to time, get a directive. In this case, two days before the new rule came out, we got a communication that said, "Oh, by the way, we're going to change the rules. We're not really sure what the rules are going to be yet, but we're going to change them." Two days later, we got the new rules, then we were supposed to implement them a few days after that.

So there's not really a build-up. There's not any indication. As I said earlier, when our Web site gets shut down in China we never get told why. We'd love to know why. We'd like for them to tell us what the rules are. But it's impossible to find out because they simply won't answer the question.

Chairman DORGAN. Have you had intellectual property stolen? I understand Google has. You indicated that attacks have been made on your system repeatedly. Have you had intellectual property stolen?

Ms. JONES. Well, I'm not exactly sure what you mean by intellectual property. It could be a broadly defined term. We do know that a lot of the IP that is stolen comes from Web sites that are hosted in China, but most of the attacks on our system are designed to disable Web sites of our customers. Those tend to be human rights sites, Tiananmen Square anniversary sites, Web site blogs that discuss Tibetan monks, any of the things that the Chinese Government deems inappropriate. They rarely ask us to shut down counterfeit goods, for example, or other IP violations because, frankly,

I think they support that. Now, have we had software or other information in our systems stolen? Not yet.

Chairman DORGAN. Thank you.

Ambassador Palmer, why do you think the State Department is so reluctant in addressing this issue of the circumventable systems for which funding exists, but the State Department seems to have little interest in programming? What is your sense of State's reasons? I mean, you worked down there. For 16 years, you worked in the State Department, right?

Ambassador PALMER. Twenty-six.

Chairman DORGAN. Twenty-six years. I'm sorry.

So what could explain the State Department's behavior at this point?

Ambassador PALMER. One State Department official was quoted in the Washington Post, saying that the Chinese authorities in Beijing would be, to use my previous word, appalled, would be outraged, if the Global Internet Freedom Consortium's systems were financed by the State Department. So it's clear, from talking to my friends both in the State Department and in the White House, that one of the concerns that has led to this is concern about the Chinese reaction.

Chairman DORGAN. So this is an old story, isn't it? Don't offend them.

Ambassador PALMER. Right.

Chairman DORGAN. We see this routinely in trade negotiations, but it's an old story and now surfaces with respect to this issue.

Ambassador PALMER. Then there's another issue, I believe. That is that the Department didn't ask for this money, didn't want this priority. It feels put upon. It still doesn't recognize that we have this long-term challenge in front of us that's going to require, year after year, major resources of financing and human talent, and they're just not into that yet. They haven't made that transition conceptually.

Chairman DORGAN. Ms. Hom, you, at least with respect to one Chinese citizen, Liu Xiaobo, put a human face on the victims here whom might be targeted by the requests made of Go Daddy to describe who these people are, names, photographs, et cetera. I assume that what the Chinese are attempting to do with that is to intimidate and to track down certain dissidents in China who are behaving in ways that the Chinese Government finds inappropriate.

But can you tell me, what's your sense of how many citizens in China have been tracked down by their government, apprehended, tried, sent to prison for Internet transgressions?

Ms. HOM. Your question is related to the overall lack of transparency about numbers in the criminal justice system and in the extrajudicial detention system, including reeducation through labor [RTL] and other detention camps. It's very difficult to answer because statistics about the total number of detentions are not reported in a comprehensive, clear way.

However, if you just look at one area, as we have looked recently, with an eye toward detentions related to Internet activities, if you look at a list of individuals in prison or in detention, or convicted for incitement to subvert state power, subversion, or for leaking

state secrets, it would be quite clear that a great majority of them will have engaged in activities on the Internet.

The draft revised state secrets law that was released in June made it clear that the state secrets law provisions apply to the Internet, including activities of disseminating and acquiring information. So the proposed revisions would make the current law more restrictive of freedom of expression on the Internet.

Chairman DORGAN. Mr. Black, you are involved in, among other things, a substantial amount of commercial transactions by your member companies. I'm wondering whether the censorship and regulation of the Internet in China has an impact, and if so, how, on companies that wish to sell goods in China?

Mr. BLACK. Yes. We are convinced that this is an important avenue to pursue, not only because it is important but because existing trade agreements, and possibly future trade agreements we will negotiate, will be able to deal with some of these issues in an already established legal framework.

I think the easiest example is any Web site, frankly, that is blocked, that Web site, in the modern Internet era, has a variety of companies—it could be automobile companies, could be Proctor & Gamble—who advertise there, who are there but are unable to adequately reach an audience if they're blocked.

There could be, if you have a magazine article, if you go to a Business Week site and there's an article in Business Week that is politically untenable, well, theoretically all of the advertisers in Business Week, all those companies would in fact have their ability to do commerce affected.

We think the reality is, that electronic commerce is a multi-billion-dollar business activity, perhaps a trillion-dollar one. So if you have a significant impact on the communication of data and information on our products and services, you are going to be having a significant impact on trade, yes.

Chairman DORGAN. Mr. Black, is there a tension for you to come here and speak on these issues? I mean, there are some in the business community—not all, but there are some—who think, you know what? It's a whole lot better for us to kind of tone it down a little bit, be quiet, hope things improve, don't be critical, because the fact is, China is a big market and the Chinese Government can just make the decision to change, limit, or close your access to that market. So isn't there a tension for you to come and speak out? I am talking about a tension with respect to your constituency and your foundation, or your association, rather.

Mr. BLACK. Well, I think it's clear that within the private sector there are many companies, which also internally are divided on how to deal with doing business in regimes where local laws conflict with our values, yes. But I think——

Chairman DORGAN. But over time, if I might interrupt you, there have been many occasions in this country where we say, you know what? Business is business. The rest, we will deal with later. Business is business and human rights is separate.

Mr. BLACK. Well, I think these issues are way beyond the Internet and technology issue and affect all businesses. But I guess I'd probably put a good word in for the technology and Internet world. I really do think the culture of our sector of the industry is one of

openness and freedom, and I think there's a greater willingness, therefore, to say that is what we are about. We are not just about selling something, but we are about using this tremendous great industry to advance people's well-being.

But yes, you are absolutely correct. There is certainly a constant pressure, not necessarily on me, but internally in the corporate dialogue, about how to deal with this problem, and with the reality that it can have a significant impact on stockholders, on the ability of a company to survive.

Chairman DORGAN. I want to ask a question of the representative from Google, and perhaps Go Daddy as well. You have both now announced that you are changing the way you operate in China. I'm going to first ask Google. Number one, I assume some think you are just daft, right? I mean, what are you thinking about?

Mr. DAVIDSON. Yes.

Chairman DORGAN. You're there, you do business. You don't like it, but you follow the local customs. Tough luck. So stop crying and move on. You're setting a bad example for those that decide business is business. You're messing things up for us within the Chinese market. Do you hear others say that?

Mr. DAVIDSON. Well, I think every company has to make its own decisions about how to operate. I think we have made no secret that this has been a difficult decision and process for Google, and we went into the market originally hoping that we could make a big difference.

We were pleased, I think, initially about some of the changes we were able to bring to the market, and ultimately over time, as we described in our testimony, we came to a different conclusion about what was right for our business. We have gotten some good feedback and our hope is that this is a process where other companies will also get involved. We need more help in the GNI.

Chairman DORGAN. So you're hoping to start a trend here?

Mr. DAVIDSON. Our long-term hope is the same hope we've had, which is that we can offer our services in China.

Chairman DORGAN. Let me ask, tell me how you think this plays out at this point. You're an executive with a big, successful, growing, worldwide company. We read the news at the moment right up to the moment, as Ms. Hom indicated. So we know what has happened so far and we know the discussion about the move to Hong Kong. But tell me how you see this playing out in the end for your company.

Mr. DAVIDSON. I think we've been very clear also: we don't know how it will play out. We have moved our servers to Hong Kong.

Chairman DORGAN. Can you give me the best and worst case?

Mr. DAVIDSON. Sure. I think one of the better-case scenarios is that people in China are able to access our uncensored search engine based in Hong Kong and have access to all the information that it provides. I think a bad-case scenario would certainly be that that search engine is blocked outright and that other services are as well, and that others rush in to fill the void with censored products that don't provide a lot of information to Chinese users. Our hope is that, over time, it will be more of the former.

Chairman DORGAN. All right. One final question and then Senator LeMieux will ask a question.

Ms. Jones, the decision Go Daddy has made, that's a very recent decision I assume, you announced today. Can you tell me the thinking that went into that decision? Is it related to Google? Tell me the judgment. I know you've talked about the attacks and you talked about the increasing demands by the Chinese Government. All of that has happened recently, so this puts you in a decision-making point here?

Ms. JONES. Well, with all due respect to Google, it really didn't have anything to do with them. This was a decision we made in our own right based on our experience of having to contact Chinese nationals, collect their personal information, and grudgingly return it back to Chinese officials. We just made a decision that we didn't want to act as an agent of the Chinese Government, and that's really why we stopped offering the .CN domain name. Honestly, we wish that there were a better way to negotiate.

In fact, you know what? I read a book once called "Take This Job and Ship It," and I remember there was a discussion in it about an unequal playing field in negotiations between the United States and other countries, and I think we ought to revisit that discussion because we can't let them be strong and us be weak all the time. We just have to stop it, and then we'll start offering .CNs again.

Chairman DORGAN. Are you recommending people read that book? [Laughter.]

Ms. JONES. Sure.

Chairman DORGAN. Full disclosure: that's a book I wrote. But I think it does raise the question of the kind of negotiations that should exist.

Senator LeMieux, let me ask you to inquire.

Senator LEMIEUX. Thank you, Mr. Chairman. I think we all should read that book. It's a great idea.

Well, again, I want to commend you, Mr. Davidson, Ms. Jones, your companies, for the work that you're doing. It occurs to me, Mr. Chairman, that if there were attacks on the bricks and mortars of these businesses and we believed that a government was behind them, we'd be acting a lot differently. We need to be cognizant of the fact that this is not just something out in the ether, it is the way that you do business. We treat it differently when it's in the ether than we do if it was bricks and mortars.

Mr. Davidson, I want to ask you about these cyber attacks in mid-December 2009 and learn more from you about what happened and where you think those attacks were directed from.

Mr. DAVIDSON. Well, sure. We tried to lay it out a little bit in our public statements and in our testimony. I'd be happy to amplify further also afterward if it's helpful for you and your office. I guess I would best characterize it as quite sophisticated and very unusual.

As we tried to explain and as Ms. Jones has explained, companies like ours are attacked all the time, but this was quite different because of the sophistication, because of the fact that we discovered that other companies had been targets, and that we also knew that part of the target seemed to be the ability to access G-mail accounts, and particularly we knew that G-mail accounts had been

compromised for folks who are affiliated with human rights groups in China or working on Chinese issues.

So that was very disturbing to us, and I think that's part of why we felt it was so important to make a change in our policy, but this is really part of an ongoing process over the course of a year.

Senator LEMIEUX. Do you believe the Chinese Government was behind the attacks?

Mr. DAVIDSON. We have no evidence, and we have not said, that we believe this. We have no evidence that this is a state-sponsored attack. We may never know. Google may never know who ultimately was behind this attack, but that's partly why this is really about a totality of circumstances over the course of a year, where Google was blocked. YouTube has been blocked in China since March, the Green Dam activities over the course of a summer, public attacks on Google in the media, this cyber attack in December.

I think, taken all together, we felt it was time for a change in our policies.

Senator LEMIEUX. I can see your legal training in your response to that question. [Laughter.]

I am a fallen engineer, if that counts for anything.

Chairman DORGAN. Senator LeMieux, can I just, on that point, the statement that was put out by Google on January 12 indicates the theft of intellectual property did not just involve Google, but also involved a couple dozen other companies. But also, part of the investigation, if I can quote: "We have discovered that the accounts of dozens of U.S.-China Europe-based G-mail users who are advocates of human rights appear to have been routinely accessed by third parties," and so on.

I mean, when you ask who might have been responsible, the obvious question is, who would have had an interest in this sort of thing? It appears, to the outsider at least, that only the Chinese Government would have this kind of interest. I am not asking you to answer that, because I'm sure you don't want to. [Laughter.]

Senator LEMIEUX. Let me ask, Ms. Jones. You described that there were cyber attacks on Go Daddy as well.

Ms. JONES. Yes. The December attack, of course we were involved in that. As I said, we have had a couple of dozen since the first of the year as well. What stood out to us about the December attack, again, was the sophistication, the level of organization, the way the traffic was routed to us. We don't know who did it, but we will go so far as to say it was quite sophisticated and there were resources behind it from somewhere.

The difference between the attack on our system and the attack on Google's system appears to be, the Google attack was aimed at infiltrating e-mail accounts. The attack on our system was designed to disable Web sites that somebody doesn't like.

Senator LEMIEUX. Yes, sir?

Mr. DAVIDSON. I don't want to be too cute with my answer, sir. I would just say it is actually a very complex environment there. There are lots of different groups that operate, nationalist groups, groups that do things. So it really is the case that we don't know, and it is also the case that I think there were a whole set of circumstances, starting with the fact that in 2006 we would be continually evaluating these circumstances and doing business that led

to our decision, but I will leave it to others to draw their own conclusions.

Senator LEMIEUX. Let me ask that question of Ms. Hom, if she has an opinion as to where these attacks are coming from.

Ms. HOM. I think that it's important not to get fixed on the question of whether it's the Chinese Government behind the attacks. It is true that in a number of these attacks, particularly against human rights groups, including Tibetan groups and some Falun Gong groups, the attack control server has been traced back to control servers located inside China. However, the real issue is the responsibility of a government in terms of cross-border crimes. So I would say that it's important that China has an obligation to investigate and to ensure that those responsible for these attacks are held fully accountable.

Mr. Davidson said that China is a complex environment. I think it's also true that when we say "the Chinese Government" we have to keep in mind it's not monolithic. In the IT Internet area there are turf battles between the different ministries, for example, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the Ministry of State Security. So in the current negotiations with Google, it may not even be clear who and what interests are represented at the negotiating table. I would guess it is a complex negotiation.

In the discussion about cyber attacks, and the technical solutions that have to be developed, we need not only access and circumvention tools. We need safe, secure, and anonymous access, access that ensures that our identity is not compromised.

Therefore, I would add to Ambassador Palmer's call for the need for more support for the development of a suite of technology tools. I don't think any one tool alone is going to work. DRL [Bureau of Democracy, Human Rights, and Labor] and the State Department has issued and closed an RFP [Request for Proposal] for the development of new mobile technologies, but it is a very limited pot and many groups have applied.

There needs to be a lot more resources devoted to the development of technology solutions. This will require governments and the donor community to step up to the plate. Unfortunately, some private donors that are trying to maintain their presence in China are moving away from supporting work, including human rights work, that might be perceived as sensitive by the Chinese authorities. Yet there is a very important role and need for support for human rights-related technology development, coming from government as well as the private sector.

Senator LEMIEUX. Mr. Black or Ambassador Palmer, do you care to take a shot at that?

Mr. BLACK. Yes. First of all, we would endorse the—what has just been mentioned. We think, to the extent you can have technological assets to bring to bear in this battle, that's great. I think it's important and valuable. It is, nevertheless, going to be a difficult fight when you are in a fight with a government with the tools governments have available. So again, we do think it is important to engage at the governmental level.

What I would suggest is—and while we all recognize, I think, that China has the most sophisticated firewall and technological

assets that they bring to bear in this area, and thus make it a more difficult problem—they are not the only country we want to focus on. I would suggest, while not de-focusing on China, that we also focus on some other countries where we may have the greater opportunity to use leverage and create some precedents that then can be turned back and used on others.

We have identified Burma, Tunisia, Thailand, Uzbekistan, Vietnam, Egypt, Turkey, Iran, and I have a longer list of countries who are doing very clear things which we think are violations of not just Internet freedom conceptually, but could be actionable under trade agreements.

I understand the U.S. Government, for various reasons, is reluctant to pick a big fight, maybe at any given point bring a trade case against China or do other things, but some of these countries we may well have some influence with and they are members of the WTO. Those rules can work for us at times.

I think if we create a pattern of precedents and create, in essence, a climate that makes China even more clearly the outrider, the outlier on this, I think in the long run that may well be more effective. Confrontation may work sometimes. We all know confrontation sometimes makes it harder to do things. But coming in from the side and from other places globally, I think, is an avenue that really can actually begin to make some progress.

Senator LEMIEUX. Ambassador?

Ambassador PALMER. On the question of who's doing this, it seems to me, clearly, obviously the Chinese Government. If you look at the history of censorship and of this kind of intervention in many countries, in dictatorships, it's always the government. Who else, as you said, Senator, has the interest? This is a sophisticated, large-scale effort. It is clear that Beijing is doing this as a matter of government policy.

On the question that Ms. Hom touched on, and that is, is there sort of a solution, a technological solution, I think the answer to that is, no, there isn't a single answer. But the State Department now, which I find really quite piquant and wonderful, is saying that they want to do venture capital. I am a venture capitalist. I have been running, and own, a venture capital firm for the last 20 years. There is a role for venture capital in this field.

I mean, it is true that in order to keep up with the engineering skills in Beijing, the Chinese skill in this, that the Communists are abusing, we are going to have to keep innovating ourselves. But it's also true in the investment world that there are products that already exist that you want to get behind with large-scale investments because they're proven and they're beyond the R&D phase. They're beyond the venture capital phase.

That is the case with the Global Internet Freedom Consortium, which is already serving all together several million people on a daily basis. If they only had the servers, they could serve 50 to 100 million people on a daily basis. It would be criminal, in my judgment, to wait to find some brand-new, sexy little thing out there that may take five more years to develop and not go ahead right now and build up an existing, proven system and devote some money. We should not devote 100 percent to the existing proven;

I'd be opposed to that. But spend serious money to build up, to scale up an existing proven system.

The only other potential competitor is Tor, which was partly developed by the U.S. Government. Tor has, in my judgment, about one-tenth as many users, but that's not insignificant either. So I think there may be two build-up possibilities that exist today, along with the R&D stuff.

Senator LEMIEUX. Well, thank you, Ambassador. Thank you for your candor. It seems to me that it's hard to imagine, Mr. Chairman, that there could be an entity inside of China that was not controlled by the Chinese Government that would be sophisticated enough to bring these attacks forward.

I have one last question, if I may, that I wanted to direct to our friends from Google. That is, you have a lot of employees, as I understand it, in China. I want to know, because I saw how this announcement was made on the blog, and there seems to be a reference to your employees. Do you have a concern about their safety?

Mr. DAVIDSON. Of course we have a concern. That's why——

Senator LEMIEUX. Beyond the normal security you have for employees.

Mr. DAVIDSON [continuing]. Right. Sure. I think it is very important to us, and that's partly why we made this announcement in January, but we took action this week. It was important for us to do this in an orderly fashion that was really sensitive to the employees that we have on the ground. We made it clear in our announcement that these decisions have been made entirely by Google executives in the United States without the involvement of our employees in China.

I think going forward, our hope is that they'll continue to be there and that they'll continue to be able to contribute. We have some fantastic engineers. We have an R&D center and a sales force there, and we'd like to continue to grow that great group of employees. But we will be watching the situation on the ground very carefully.

Senator LEMIEUX. Mr. Chairman, I want to thank you again. I think that you have brought a lot of light and attention to this issue by chairing this hearing today. I want to thank all the witnesses for being here.

As I said in my opening statement, with great power comes great responsibility. We need for the Chinese Government to stand up and not have the censorship anymore. I believe that the Internet is going to be the greatest tool of the modern time to promote communication, and eventually democracy, throughout the world. I applaud both of your companies, again, for the good work that you're doing.

Thank you, Mr. Chairman.

Chairman DORGAN. Senator LeMieux, thank you very much.

Mr. Ambassador, when you began today you said some encouraging things about China. Most, however, of the rest of this hearing has been rather discouraging when we're talking about Internet freedom, censorship, people going to prison. So tell me again, what do you see for China? You've watched diplomatic issues and worked in the State Department 26 years.

What do you see going forward here? I mean, it's pretty clear, it seems to me—and everybody in the room—however critical one might be of China, all of us understand that things in China are marginally better. Things have improved over the last 25 years in a number of areas. However, there are many other areas where you still have the authoritarian fist of a regime that wants to protect itself.

As you answer this, let me ask you, looking at the regimes in Eastern Europe that prevented their citizens from hearing and seeing what was happening in the rest of the world, my understanding is the landscape changed with the introduction of the video cassette recorder [VCR].

When the VCRs came in and video cassettes could be moved around the world, people in their living rooms in Eastern Europe could run a cassette and watch a movie or see programming. It was impossible for those governments to prevent information from getting to people.

The Internet, of course, is the video cassette recorder on super steroids, right? How effective can the Chinese Government be regarding censorship, given the power of the Internet? What is your impression? I'm sorry for the lengthy question.

Ambassador PALMER. No. I think that's absolutely right, they will not succeed. It is simply impossible in a modern society, which China increasingly is a modern society, an extraordinary society which has been transformed in the last generation. It's a totally different country. It is impossible. I spent much of my foreign service career living in Eastern Europe and we learned the power of rock and roll, not only video cassettes, but rock and roll.

I mean, you know, kids are kids and they don't want this nonsense. They're skeptical of the political leaders and they are the children of the leaders, and the nephews and nieces. Over the dinner table, they tell some homely truths to the people who live in Zhongnanhai, to the leadership of China. So I see so much evidence that we're basically winning.

I mean, when you have 11,000 people with their own names sign Charter 08, which is the most important written document in modern Chinese history—not since Sun Yat-sen founded modern China has there been a piece of paper more explicit, clear, and more powerful than that is. And 11,000 of the leading people in the country—what we learned in Eastern Europe is that among elites, when things look so dark, there is a whole lot of foment going on.

I just finished reading Zhao Ziyang's book when he was the General Secretary of the Communist Party of China at Tiananmen. He's written a book. He dictated, in secret, his memoirs before he died. It's called, "The Prisoner of the State," and I would recommend everybody to read it. He and his predecessor, Hu Yaobang, who was the previous General Secretary of the Communist Party, after all—I mean the top party official in the country—both of them wanted ultimately complete democracy in China, with everything that we call a democracy.

So when you've got really senior people, now you can see what their thinking was, I am certain that today in Zhongnanhai you have all kinds of people who recognize that this oppression of

Google is a mistake and they don't want it. Eventually they will be the rulers of the country.

Chairman DORGAN. Let me, in conclusion, ask a question of both Google and Go Daddy. The decisions you have now made, are these decisions for the moment, interim decisions, or are there things the Chinese Government can do that would convince you that that decision should be modified or changed? Give me your assessment of where you are now relative to conditions in China and what the Chinese Government might or might not do that would change these decisions.

Mr. DAVIDSON. Well, I would say our hope is what it's always been, which is to be able to offer our services and access to information to our users in China. If, tomorrow, we were able to offer an uncensored version of our search engine in China, we would absolutely consider that. I think that would be a welcome move.

But throughout our conversations the Chinese Government has indicated that that's not a negotiable point, so we are where we are. Our hope is that the way we've done this, the solution we've put forward, operating out of Hong Kong, will be a way that will give people access to information, and over time they will.

If I could actually, just to amplify the point that the Ambassador just made, to just say that I think we actually do have a little bit of a hard road ahead. In the mid-1990s there was this great saying floating around the Internet that "the Internet interprets censorship as damage and routes around it." That was John Gilmore, who's an engineer, not a lawyer. It was this great idea, that the Internet was this unstoppable force for freedom. If you have the Internet, you can't stop people from getting information.

What we've discovered, and I think the point in my testimony was, that in the last 15 years governments have started to learn how to exert more control and it's going to take a lot of work to combat that censorship. But I am an optimist, as well I think we are optimists, that human nature demands information, that people will seek information regardless of frontiers, to paraphrase the UN Declaration of Human Rights, and that ultimately that Internet freedom will be something that we'll be able to achieve. But it's going to take a lot of work and we need your help.

Chairman DORGAN. All right.

And Ms. Jones, what do you believe is Go Daddy's future relationship with business in China?

Ms. JONES. We would say something similar. We have been doing this for six years. We see no reason why we shouldn't continue to do it for six more, and six more after that. But again, we have to have a reasonable expectation from officials in China as to what level of information is going to be required. If they want to go ahead and repeal the new rules, we'll probably open up the .CN name the next day. It's just a flip of a switch for us.

But it's really discouraging to us that we've been able to help people in China get their message out for six years, and then suddenly, in the snap of a finger, the service has to become unavailable because it looks like we need to operate, as I said before, as the agent of the Chinese Government, and we're not interested in being that.

We really exist to enable people to share their thoughts openly and we agree that the Internet demands the open exchange of ideas. Some of them are good and some of them aren't, but nevertheless they are all ideas and they deserve to be shared. So we would strongly urge this Commission to work with the authorities in China to repeal that rule, and if you can accomplish that we'll be happy to flip the switch and turn it back on.

Chairman DORGAN. Well, thank you very much.

Let me thank all of the witnesses. Senator LeMieux, thank you for your participation. I'm just looking at this CECC document that our Congressional-Executive Commission on China will be putting in the record today of political prisoners in China, with their photographs and data. These are people who have gone to the Internet and published articles and journals, and for that they are sitting in a dark prison cell somewhere in China.

It demonstrates that this issue is not just some theoretical issue over which we should just have an interesting discussion or debate. It is, in some cases, life and death, and it is always about freedom. This Commission scheduled this hearing to try to understand what is happening in China, especially as a result of the Google decision. Again, I compliment Google and compliment Go Daddy for making decisions that I'm sure are difficult to make, but yet reflect companies that are willing to make the right decisions.

It is our hope that things in China will improve. It's not our lot in life to decide that we should just beat up on China every time we have a hearing, but China is going to be a big part of our future. It's a significant, important part of the world. And, it's going to be a significant, important part of the future of our country, the United States. If not for that reason alone, we must examine what is occurring inside China today.

It has always been our intention, especially through trade, travel, and also through information, to pursue what is called "constructive engagement" with China and similar countries, believing that constructive engagement would move these countries toward greater respect of human rights. Yet, we find ourselves, in March 2010, still talking about a country that censors the Internet and throws people into the dark cells because of what they think or what they publish. This behavior by a state seems so out of touch with the modern world.

Today the Commission engaged a discussion about Internet freedom in China and how we might persuade that country to move toward greater human rights. So all of you have contributed significantly to the hearing, and we appreciate your testimony and your attendance.

This hearing is adjourned.

[The questions and responses submitted for the record appear in the appendix.]

[Whereupon, at 3:53 p.m. the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENTS

PREPARED STATEMENT OF ALAN DAVIDSON

MARCH 24, 2010

Chairman Dorgan, Chairman Levin, and Members of the Commission.

Thank you for bringing attention to the important issue of Internet censorship, and for giving Google the opportunity to discuss today's global challenges to freedom of expression and access to information online. Internet censorship is a growing global problem. It not only raises important human rights concerns, but also creates significant barriers for U.S. companies doing business abroad. As Google's Director of Public Policy in the Americas, I am part of the Google team that works to promote free speech both in the United States and globally.

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

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

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

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

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

With those principles in mind, we would like to address four main issues in this testimony:

First, Google's situation in China.

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

Third, the economic implications of censorship.

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

CHINA UPDATE

Let us start with an update on Google's situation in China.

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

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

However, in the last year we have seen increasing attempts to limit free speech on the Web in China. Numerous sites including YouTube, The Guardian, Facebook,

Twitter, Blogger and Wikipedia have been blocked, some of them indefinitely. In addition, last June the Chinese government announced that all personal computers sold in China would need to be pre-loaded with software that could be used to censor online content. After a public outcry and pressure from companies, the proposal was later withdrawn.

Most recently, in mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China. What at first appeared to be an isolated security incident—albeit a significant one—turned out upon investigation to be something quite different.

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

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

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

The attack on our corporate infrastructure and the surveillance it uncovered—as well as attempts over the past year to limit free speech on the Web even further—led us to conclude that we were no longer willing to censor our search results in China. This decision was in keeping with our pledge when we launched Google.cn that we would carefully monitor conditions in China, including new laws and other restrictions on our services.

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

Earlier this week we stopped censoring our search services—Google Search, Google News, and Google Images—on Google.cn. Users visiting Google.cn are now being redirected to Google.com.hk, where we are offering uncensored search in simplified Chinese, specifically designed for users in mainland China and delivered via our servers in Hong Kong.

Figuring out how to make good on our promise to stop censoring search on Google.cn has been hard. We want as many people in the world as possible to have access to our services, including users in mainland China, yet the Chinese government has been crystal clear throughout our discussions that self-censorship is a non-negotiable legal requirement. We believe this new approach of providing uncensored search in simplified Chinese from Google.com.hk is a practical solution to the challenges we've faced—it's entirely legal and will meaningfully increase access to information for people in China. We are well aware that the Chinese government can, at any time, block access to our services—indeed we have already seen intermittent censorship of certain search queries on both Google.com.hk and Google.com.

In terms of Google's wider business operations, we intend to continue R&D work in China and also to maintain a sales presence there, though the size of the sales team will obviously be partially dependent on the ability of mainland Chinese users to access Google.com.hk.

Before moving on to the broader, global challenges Google faces, we would like to make clear that all these decisions have been driven and implemented by our executives in the United States, and that none of our employees in China can, or should, be held responsible for them. Despite all the uncertainty and difficulties they have faced since we made our announcement in January, they have continued to focus on serving our Chinese users and customers. We are immensely proud of them.

OTHER GLOBAL CHALLENGES AND ECONOMIC IMPLICATIONS

China is simply one example of a global phenomenon that raises concerns. Google has become a regular focus of governmental efforts to limit individual expression because our technologies and services enable people with Internet connections to speak to a worldwide audience.

More than 25 governments have blocked Google services over the past few years. Since 2007, YouTube has been blocked in over a dozen countries. We have received reports that our blogging platform has been blocked in at least seven countries, and that our social networking site, Orkut, has been blocked in several countries.

Iran provides a prominent recent example of political censorship. This past June, during the protests that followed the presidential election in Iran, the government

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

The Iran example demonstrates why it's imperative for governments, companies, and individuals to do more to ensure that the Internet continues to be a powerful medium for expressing political opinions, religious views and other core speech without restriction.

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

When a foreign government pursues censorship policies in a manner that favors domestic Internet companies, this goes against basic international trade principles of non-discrimination and maintaining a level playing field. Local competitors gain a business advantage, and consumers are deprived of the ability to choose the best services for their needs. And when a government disrupts an Internet service in its entirety—e.g., blocking an entire website because of concerns with a handful of user-generated postings—the government is restricting trade well-beyond what would be required even if it had a legitimate public policy justification for the censorship.

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

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

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

HOW GOVERNMENTS CAN SUPPORT FREE EXPRESSION

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

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

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

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

from government officials; and greater engagement by the U.S. Government with countries that censor the Internet, so any company disclosures result in concrete actions by the U.S. government.

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

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

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

On the multilateral human rights front, enforcing and supporting the mechanisms of the International Covenant on Civil and Political Rights and others under the UN system (e.g., the UN Human Rights Committee) to demand accountability from governments for Internet censorship is helpful. At the very least, these mechanisms can be better used to shine light on government abuses.

CONCLUSION

We would like to thank Chairman Dorgan, Chairman Levin, the members of the Congressional-Executive Commission on China, and other Members of Congress who have spoken in support of upholding the right to online free expression around the world. It is only with the attention and involvement of leaders like yourselves that we can make real progress in the effort to protect these basic human rights. We look forward to working with you and other government officials to find viable solutions to maximize access to information, increase transparency and protect users around the world.

PREPARED STATEMENT OF CHRISTINE JONES

MARCH 24, 2010

INTRODUCTION

Thank you, Chairman Dorgan, and members of the Commission, for the honor of testifying here today. We at Go Daddy applaud the actions of the Commission to support the continuing global exchange of information and trade on the Internet.

BACKGROUND

The recent cyber attacks on Google and other U.S. companies are troubling, but they reflect a situation that The Go Daddy Group has been combating for many years. Go Daddy is an Arizona company which consists of eight ICANN-accredited registrars, including GoDaddy.com, Inc., the world's largest domain name registrar. This month, Go Daddy passed a major Internet milestone—we now have more than 40 million domain names under management, more than any other company in the history of the Internet. We are also the largest provider of shared website hosting. We have more than 7 million paying customers located all over the globe. So, if you are an active Internet user with a domain name or a website, the likelihood is that at some point you have utilized Go Daddy's services to engage on the Internet.

Go Daddy's customer base includes tens of thousands of Chinese nationals. We work with Chinese customers on a daily basis to help them to establish an identity on the Internet, and to ensure the secure and seamless operation of their hosted websites. We are also constantly in the process of repelling cyber attacks against the systems and infrastructure that secure our customers' websites and Internet activities. A large percentage of those attacks can be traced to China, as can other illegal activities that interfere with our customers' safe and productive use of the Internet. I am here today to share some of our experiences as they relate to China, specifically with respect to the following: increased monitoring and surveillance of .CN domain name registrations; increasing DDoS attacks originating in China; spam; payment fraud; and, what we would like to see the U.S. Government do to help alleviate some of these issues.

INCREASED MONITORING AND SURVEILLANCE OF .CN REGISTRATIONS

There appears to be a recent increase in China's surveillance and monitoring of the Internet activities of its citizens. As a domain name registrar, Go Daddy provides registration services for numerous top level domain names. Top level domains, or "TLDs," are the suffix that appears at the end of a domain name (for example, .COM, .NET, etc.). One of the TLDs we have historically offered is .CN, the Chinese country code top level domain (or "ccTLD"). Go Daddy is authorized by the China Internet Network Information Centre (known as the CNNIC), a quasi-governmental agency in China, to offer registration services for the .CN ccTLD. Go Daddy began to offer the .CN ccTLD in April of 2005 and, at this time we have approximately 27,000 .CN domain names under management. Registering a domain name with the .CN ccTLD is an important step for any individual or company wishing to establish an audience or business foothold in the Chinese market.

When Go Daddy started registering the .CN TLD in 2005, CNNIC required us to collect the contact information of the individual or company registering the domain name. The required contact information included first and last names of the registrant, his or her physical address, telephone number and email address. The extent of the personal information collected was typical of what is normally required by .ccTLD registries.

A little over four months ago, on December 12, 2009, CNNIC announced that it was implementing a new policy relating to the registration of .CN domain names, and that it would begin to enforce the new policy effective December 14, 2009. The policy required that any registrants of new .CN domain names provide color headshot photo identification, business identification (including a Chinese business registration number), and physical signed registration forms. This information was to be collected by the registrar, and then forwarded to CNNIC for its review prior to the activation of the registration.

Less than a month later, on January 5, 2010, CNNIC announced that Chinese nationals were no longer permitted to register domain names through non-Chinese registrars. In accordance with the new policy, Go Daddy halted all new .CN registrations.

On February 3, 2010, CNNIC announced that it would reopen .CN domain name registrations to overseas registrars. However, the stringent new identification and documentation procedures would remain in effect. CNNIC also announced an audit of all .CN domain name registrations *currently* held by Chinese nationals. Domain name registrars, including Go Daddy, were then instructed to obtain photo identification, business identification, and physical signed registration forms from all *existing* .CN domain name registrants who are Chinese nationals, and to provide copies of those documents to CNNIC. We were advised that domain names of registrants who did not register as required would no longer resolve. In other words, their domain names would no longer work.

We were immediately concerned about the motives behind the increased level of registrant verification being required by CNNIC. It did not make sense to us that the identification procedures that had been in place since 2005 were apparently no longer sufficient from China's standpoint, and no convincing rationale for the increase in documentation was offered. We were also concerned by the *ex post facto* nature of the new requirement—in other words, at the time the affected Chinese nationals registered their domain names, they were not required to provide photo identification and the other documentation now being required by the CNNIC. The new documentation requirement was to be retroactively applied to registrants who had previously registered their websites, in some cases years before. The intent of the new procedures appeared, to us, to be based on a desire by the Chinese authorities to exercise increased control over the subject matter of domain name registrations by Chinese nationals.

Approximately 1,200 unique Go Daddy customers were affected by CNNIC's *ex post facto* application of the requirement for additional identification documentation. This represented a much larger number of domain names, of course, because many registrants have multiple domain names under their control. We contacted our affected customers advising of this new requirement, and advised them that, if they wished to provide us with the required documentation, we would provide it to CNNIC in accordance with CNNIC's directive. Ultimately, only about 20 percent of the affected customers submitted the required documentation and agreed to allow us to submit it to the CNNIC. The domain names of the remaining 900 or so customers remain at risk of cancellation. That means thousands of websites the Chinese authorities may successfully disable because of retroactive application of this new set of rules.

Go Daddy has been registering domain names since 2000. We currently serve as an authorized registrar for dozens of domain name extensions. This is the first time a registry has asked us to retroactively obtain additional verification and documentation of individuals who have registered a domain name through our company. We are concerned for the security of the individuals affected by CNNIC's new requirements, as well as for the chilling effect we believe the requirements will have on new .CN domain name registrations. For these reasons, we have decided to discontinue offering new .CN domain names at this time. We continue to manage the .CN domain names of our existing customers.

INCREASING DDOS ATTACKS ORIGINATING IN CHINA

Another China-related issue we have seen recently is an increase in the number of distributed denial of service (also known as "DDoS") attacks on the systems that host our customer websites. In Go Daddy's case, a DDoS attack is typically an attempt to make websites that we host unavailable to their intended users for some period of time. We also combat many attacks that are more systematic, such as hackers attempting to insert malicious code into the pages of our customers' hosted websites. An example of this type of attack would be the installation of spyware on the computers of all visitors to a website we host. The spyware then logs keystrokes to harvest passwords to email accounts, which can then be infiltrated and monitored without the knowledge of the account owner.

Go Daddy operates data centers, and has invested hundreds of millions of dollars in those centers, including building and operating state-of-the-art security measures that monitor and fight external attacks on our systems 24 hours a day, 365 days a year. In the first three months of this year, we have repelled dozens of extremely serious DDoS attacks that appear to have originated in China, based on the IP addresses from which the attacks derived. Had our security systems not countered these attacks, the result would have been a widespread take-down of our customers' hosted websites.

SPAM

Unlike many other Internet companies of our size, Go Daddy operates a large 24/7 Abuse Department whose mission it is to identify and help stop illegal and malicious activity on the Internet. We work very closely with local, federal and international law enforcement agencies to stop all types of Internet abuse, including child pornographers, unauthorized online pharmacies, spammers, phishers, and sellers of counterfeit merchandise.

In monitoring spam activities, we have found that an overwhelming majority of websites promoted through spam are hosted in China, often at service providers that choose to ignore complaints of spam and other types of illegal activity. When Go Daddy and other legitimate hosting companies receive complaints that spam is being sent from websites hosted by their company, the sites are typically taken offline. However, many companies in China offer so-called bulletproof hosting, where websites are allowed to stay online and spam operations can continue unabated, even after receipt of a complaint.

China is also the location of choice for buying and selling lists of spam "zombies"—personal computers deliberately infected with spam-enabling viruses and operated by ordinary, usually oblivious, computer users around the world. Our research indicates that China dominates the market for buying and selling lists of zombie PCs, which are peddled by virus writers on Internet forums found on Chinese servers. Lists can currently be had for about $2,000–$3,000 per 20,000 compromised computers.

Another reason so much spam appears to originate in China is the spam industry's growing sophistication. The modern spam industry is populated by technically advanced programmers and organized crime rings. Spammers create complex

phishing scams to lure individuals to fake websites where they are conned into divulging bank account, social security and credit card details. Organized spam groups tend to avoid operating in jurisdictions where authorities are hostile and penalties potentially severe. To date, China has not enforced significant penalties against spammers and others who utilize the Internet to engage in criminal activities; thus, it has become a sort of safe harbor for such criminals.

China is also an attractive locale from which spammers operate because of its low costs. A domain name can be bought for as little as $0.15 in China, which allows scammers to acquire lots of domain names inexpensively. Domain names cost much more in the United States, where some of the money goes to fighting abuse and spam. But the low revenue stream in China is likely hampering the creation of programs to stop abuse.

China today is basically the only major market where spammers can do just about anything they want. Go Daddy's efforts to persuade authorities there to investigate or prosecute spammers have been ineffective, as have our efforts to work with Chinese-based hosting companies to shut down compromised websites. Official pronouncements by the Chinese government usually appear to be aimed at getting Chinese spam servers removed from foreign blacklists rather than actually preventing spam.

PAYMENT FRAUD

In addition to our Abuse department, Go Daddy also has a full time Fraud department that is continually monitoring and guarding against payment fraud issues affecting our customers. The payment fraud trends associated with China-based users include the widespread use of compromised U.S. or UK credit cards to purchase items. In one particularly egregious case, an individual or group operating from China is utilizing compromised credit cards from a wide variety of banks to purchase one year domain name registrations. The registrant then attempts to use the domain names to perform a variety of illegal activities. Since January, our Fraud team has managed to close 134 new shopper accounts associated with this repeat Chinese fraudster.

Go Daddy has also been successful in combating Chinese spammers by closing customer accounts through our payment fraud process. Most recently, our Abuse department identified a Chinese-based spammer with 175 separate shopper accounts with Go Daddy. Although each of the accounts was opened using a valid PayPal account, we were able to halt the spammer's activities by placing a payment fraud lock on the accounts.

In addition to the challenges presented by China-based criminals, societal and cultural norms in China can make it difficult to identify and resolve payment fraud issues affecting legitimate Chinese customers. For instance, a problem we frequently encounter is the provision of invalid shopper/billing information by Chinese shoppers. Where invalid information is provided, contacting the customer to verify order activity is usually impossible.

Credit card use is not prevalent in China, and most Chinese shoppers do not possess their own credit card. When credit cards are issued, they are often shared by numerous individuals. It is therefore very common for accounts owned by Chinese shoppers to have multiple unrelated names and addresses on file. This too makes identifying payment fraud more difficult.

Despite these payment fraud challenges, Go Daddy is focused on continuing to serve and expand upon its Chinese customer base. In furtherance of this goal, in December 2009, we began to offer the Alipay payment processing system to our customers. Alipay is China's leading independent third-party online payment platform, with more than 270 million registered users. What sets Alipay apart from other online payment platforms is that it holds funds in escrow until the product is received. Chinese customers can fund their Alipay accounts using direct bank payments or debit cards, both of which are more common forms of payment in China than credit cards. Alipay is a popular and trusted option for Chinese consumers, and we have experienced a large increase in our volume of sales to Chinese customers since we implemented it as a payment option. We have also found use of the Alipay system to be very helpful in combating China-related payment fraud. In fact, our new shopper payment fraud rates associated with Chinese accounts has been reduced by approximately 50 percent since we introduced Alipay in December of 2009.

WHAT THE U.S. GOVERNMENT CAN DO TO HELP

Go Daddy's primary mission is to promote secure, easy, equal access to the Internet to people around the world. We are also committed to ending illegal or nefarious uses of the Internet, including for the invasion of personal privacy or to limit free-

dom of expression. We believe that many of the current abuses of the Internet originating in China are due to a lack of enforcement against criminal activities by the Chinese government. Our experience has been that China is focused on using the Internet to monitor and control the legitimate activities of its citizens, rather than penalizing those who commit Internet-related crimes.

We believe that countries or individuals that engage in cyber attacks or other types of Internet crimes should face serious consequences and international condemnation. We hope that the U.S. government can use its influence with authorities in China to increase Chinese enforcement activities relating to Internet abuse, while encouraging the free exchange of ideas, information, and trade. This would include the retraction of China's recent policies relating to the registration of .CN domain names, which will act as a barrier to Internet access by Chinese nationals.

PREPARED STATEMENT OF SHARON HOM

MARCH 24, 2010

Mr. Chairman, thank you for inviting Human Rights in China (HRIC) to testify at this important and timely hearing. As a Chinese human rights NGO, HRIC appreciates this opportunity to share our experience and some modest recommendations. In light of the events of the past week, the topic for today is a story still in progress.

The loss of annual MFN review leverage in 2000 and a decade of delinking of human rights from trade has contributed to the lack of systematic and sustainable human rights progress, and an unstable, unpredictable climate for foreign business in China. In recent months, there have also been disturbing reports about a series of cyber-attacks, including the one publicized by Google in January of this year, emanating from China, targeting foreign governments, private businesses, and human rights advocates both in the United States and around the world. These cyber-attacks present serious cross-border human rights, diplomatic, and business challenges for China and the world.[1]

As the comprehensive CECC Annual Report for 2009, the State Department Country report for China, and recent United Nations human rights reviews of China's record demonstrate, human rights violations in China—a country vital to U.S. security, trade, and human rights policy interests—remain serious, systematic, and widespread.[2] On top of the economic, political, and increasing soft power leverage of China, China exerts control over expression on the Internet through its state-of-the arts technology, state secrets and state security system, police and security apparatus, and resulting self-censorship.[3] By doing so, the Chinese government's policy and practices on information control implicate two universally recognized and mutually reinforcing human rights—the right to freedom of expression and opinion and the right to privacy.[4]

The experiences of HRIC's own staff also illustrate that the Chinese authorities' repressive tactics at home extend to Chinese nationals and human rights defenders abroad. Such tactics include blacklisting, surveillance, and even inhumane denials of permission to return to China for family funerals. Additionally, the Chinese authorities have succeeded in preventing independent human rights NGO dedicated to China from succeeding in applying for ECOSOC status or UN conferences' accreditation—thereby undermining independent Chinese NGO voices.

ROLE OF TECHNOLOGY

The rapid pace of technology developments globally and in China, including in mobile and connective technologies, has provided tools for increased social control and human rights violations in China, especially regarding freedom of expression and privacy. However, China's Great Fire Wall is impressive, but clearly not impregnable, as technology developments also provide tools for advancing fundamental rights and democracy in China. With over 384 million citizens online, 600 million mobile phone users, and between 26,000 to 30,000 Tweeters, all despite China's censorship regime, China is a prime target country for developing empowering potential uses for new technology, which will also have significant implications for the region and for the future security and viability of the Internet worldwide.

For more than two decades now, HRIC has focused on supporting Chinese lawyers, activists, journalists, writers, and other rights defenders in China. From our China office in Hong Kong, and our U.S. office in New York, and with a committed staff with Chinese and international law, technology, and media expertise, we have also been developing and deploying a range of technology approaches and tools to promote uncensored information flow into and out of China. Using Internet tech-

nology that bypasses China's censorship mechanism, HRIC has provided and continues to provide an uncensored platform for Chinese voices and disseminates independent news, discussion, and rights-related electronic publications through stable mass e-mail delivery to over 200,000 subscribers in every province and autonomous region in China.

HRIC's electronic publications provide access to proxy servers and six interrelated websites offering online Chinese publications, tools for activists, and online advocacy resources. Analysis of e-mail delivery rates indicate that since a new electronic biweekly was launched in June 2009, an average of 74 percent of biweekly e-newsletters reached the first Simple Mail Transfer Protocol (SMTP) server in mainland China. This program has enabled individuals in China, through the use of proxy technology and other circumvention tools, to have uncensored access to human rights information on the Internet and a space for debate and discussion. HRIC incorporated YouTube and Twitter into its advocacy strategy last year as well, launching an HRIC YouTube channel and regularly tweeting the latest human rights developments.

THE CASE OF LIU XIAOBO: WHO'S AFRAID OF THE INTERNET?

There is perhaps no better example of the Chinese government's anxiety underlying the official crackdown on freedom of expression on the Internet than the case of Liu Xiaobo, a prominent independent intellectual in China, long-time advocate of political reform and human rights in China, and outspoken critic of the Chinese communist regime.

On Christmas Day, 2009, a court in Beijing convicted Liu Xiaobo of "inciting subversion of state power" and sentenced him to 11 years in prison and two years of deprivation of political rights. The verdict cited as evidence passages from six essays Liu published online between 2005 and 2007 and his role in drafting Charter 08, an online petition for democratic reform issued on December 9, 2008, which has since garnered more than 10,000 signatures, predominantly from Chinese in China. On February 9, 2010, a higher court rejected Liu's appeal and upheld the verdict.[5]

Liu Xiaobo's case elucidates one of the most crucial challenges facing the emerging Chinese civil society: the clash of visions between Chinese pressing for a democratic China governed by genuine rule of law, and the Chinese authorities, who demonstrate time and again their intolerance for diverse views and their need to maintain control at all cost. The outcome of Liu's case has made clear the authorities' willingness to trample on a fundamental human right protected in the Chinese Constitution and enshrined in international human rights law. It also raises serious concerns about the prospects for the rule of law, human rights, and democracy in China.

Liu's six essays cited in the verdict were the following:

- The CPC's Dictatorial Patriotism (posted on Epochtimes.com and 5 links): Liu debunks the notion successfully purveyed by the CPC that the ruling party is the Chinese nation itself, a fallacious concept that has enabled it to maintain absolute rule over the people.
- The Many Aspects of CPC Dictatorship (512 clicks; posted on observechina.net; secretchina.com): Liu describes the post-Mao regime—unlike that during the era of "Maoist totalitarianism"—as more skillful in using "pragmatic, .exible control methods" to maintain stability. Liu warns that "[t]he loyalty bought by the promise of a comfortable life has a soul that is rotten to the core," and that the system is ultimately unsustainable.
- Can It be that the Chinese People Deserve Only "Party-Led Democracy?" (402 clicks; posted on epochtimes.com; observechina.net): Liu points out that the Chinese people—having been conditioned historically to view any benevolent policy as mercy granted by their ruler—are in fact complicit in their own oppression. Rather than waiting for the arrival of a "virtuous master," they must, Liu maintains, place their hope in the "continuous expansion of the ?'new power' among the people."
- Changing the Regime by Changing Society (748 clicks; posted on epochtimes.com; observechina.net): Liu explores how a continuously growing civil society is the key to China's gradual, bottom-up transformation into a free society.
- The Negative Effects of the Rise of Dictatorship on World Democratization (57 clicks; posted on observechina.net; secretchina.com): Liu discusses China's use of "money diplomacy" to degrade world civilization, and the necessity of helping the world's largest dictatorship transform into a free and democratic country with direct consequences for global democratization.

- Further Questions About Child Slavery in China's Kilns (488 clicks; posted on minzhuzhongguo.org; renyurenquan.org): Liu examines the extreme government corruption and lack of accountability that have enabled thousands of children to be kidnapped and used as slaves in kiln factories.

The verdict also cited Charter 08 (5154 clicks; posted on chinesepen.org, boxun.org, minzhuzhongguo.org).

Liu Xiaobo was a principal drafter of Charter 08, an appeal for fundamental political transformation and for the implementation of key foundational principles—freedom, human rights, and equality, among others. The document also lists 19 essential features of a new, democratic government, including legislative democracy, judicial independence, urban-rural equality, freedom of association, assembly, expression and religion, social security, and transitional justice.

In their argument at trial, Liu's defense lawyers pointed out that the articles and Charter 08 were posted on websites based outside China, not accessible by people inside China. However, the court's verdict provided the total number of clicks, as of December 23, 2009, on the articles and Charter 08 as 7,361 (with the clicks on specific items ranging from a low of 57 to a high of 5,154). Even if all the clicks were made by Chinese citizens inside China, and even if each click represents a different visitor, the total number of people is an infinitesimally small portion of China's population of 1.3 billion.

If 7,361 people reading these documents can, in the view of the Chinese authorities, pose such a grave threat, whatever that reveals about the sense of security among those in power, Liu Xiaobo's case is also a testament to the power and necessity of freedom of expression.

In addition to the high-profile case of Liu Xiaobo, there are countless other examples of China's use of the crime of "incitement to subvert state power" to punish expression on the Internet. Scholars, journalists, artists, lawyers, and rights activists have all found themselves prosecuted for "incitement to subvert state power," for doing nothing more than exercising their rights to freedom of expression and opinion online. As a consequence of using the Internet as a platform to speak out on such important issues as democratic reform, laborers' rights, state confiscation of lands, earthquake victims' rights, and government corruption, these individuals have been sentenced to draconian prison terms, some lasting more than a decade. In 2009, HRIC issued press releases on at least 12 individuals who had come under official scrutiny for their activities on the Internet.[6]

LOOKING AHEAD AND RECOMMENDATIONS

In the fall of 2012, the Communist Party of China (CPC) will hold the 18th National People's Congress. Due to term restrictions, Hu Jintao, the current President of the People's Republic of China, will be required to step down as the party's General Secretary at that time. The 18th National People's Congress will therefore be the first time in the CPC's history that a meeting to redistribute power will be held without a political strongman casting his shadow over it. It will decide on the dominant power in China's politics for the following five to ten years.[7]

The political contest surrounding the 18th National People's Congress is already having a clear effect on the current political situation in China. The pattern in the past has been that during the process of power transition within the CPC, various factions exhibit exceptional toughness in order to demonstrate their ideological orthodoxy and thus gain the upper hand in the power struggle. The comprehensive tightening of social controls by Chinese authorities since last year and their recent tough attitude in dealing with a series of both domestic and foreign events is a manifestation of this effect. One should not expect there to be any relaxation of this posture before the 18th National People's Congress convenes in 2012.

While the political climate for the next few years may not be encouraging, there are still concrete actions that the U.S. government and the private sector can take.

- Individual cases: In line with the U.S. government's renewed engagement with the UN Human Rights Council, the United States can press for releases of individuals as part of China's compliance with decisions of independent UN human rights mechanisms such as the Working Group on Arbitrary Detention, which has issued decisions on cases such as those of Shi Tao and Jin Haike.[8]
- Promoting empowering uses of technology: The past decades of rapid-paced technology developments in China demonstrate that there is no one silver bullet for a sustainable solution to protect freedom of expression and advance open, safe, and secure access to information, both of which are critical to development of a democratic and open society and a rule of law. Effective technology solutions must be informed by human needs and deployed using approaches that are sensitive to local culture, politics, and human rights history and traumas.

Some specific areas in which the CECC could encourage greater support and development through various existing and expanded U.S. government programs and initiatives include:

—Expanding support for uncensored multimedia platforms for Chinese voices and independent news, discussion, and rights-related information, including through creative use of social networking tools and YouTube.

—Development and safe dissemination of circumvention tools beyond the small group of sophisticated netizens already able to use these tools.

—Capacity-building initiatives that more effectively use interactive web-based conference tools to allow a greater range of targeted participants that avoid the expense, travel restrictions, and other political limitations of on-site events.

- Promote diverse, concrete solutions and approaches for doing business responsibly in China,[9] including multi-stakeholder initiatives, e.g., encouraging companies to join and help develop the Global Network Initiative. The February 2010 letter from Senator Richard Durbin to 30 technology companies asking them to join the Global Network Initiative and seeking more information about their business practices in China is one welcome step. In light of the global nature of the challenges, the U.S. should also explore joint initiatives with other governments.

The Google decision announced this week also illustrates the possibility of moving strategically beyond an either/or mentality of stay-and-censor or leave-the-country. By making its most recent move to redirect users from Google.cn to Google.com.hk, and by creating an additional website clearly and regularly updating the status of the Chinese government's interference, Google has contributed to increasing the transparency of and possible accountability for Chinese censorship. Although it's not clear whether this one-country, two systems move will evade the censorship system, at the very least, Google has taken a stand that it will no longer be complicit in Chinese government violation of human rights.

The human rights and business issues and challenges are complex, and as Google co-founder Sergey Brin stated, "The story's not over yet."

Thank you and I look forward to your questions.

---

[1] For more detailed discussion on cyber-espionage, see Ron Deibert and Rafal Rohozinski, "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor, Munk Centre, JR02–2009, March 29, 2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

[2] See U.S. Congressional-Executive Commission on China, 2009 Annual Report, available at http://www.cecc.gov/pages/annualRpt/annualRpt09/CECCannRpt2009.pdf; U.S. Department of State, 2009 Human Rights Report: China (includes Tibet, Hong Kong, and Macau), available at http://www.state.gov/g/drl/rls/hrrpt/2009/eap/135989.htm; United Nations Committee Against Torture, "Concluding observations of the Committee against Torture: China," UN Doc. CAT/C/CHN/CO/4, December 12, 2008, available at http://www2.ohchr.org/english/bodies/cat/cats41.htm; United Nations Committee on the Elimination of Racial Discrimination, "Concluding Observations of the Committee on the Elimination of Racial Discrimination: China," UN Doc. CERD/C/CHN/CO/10-13, August 28, 2009, available at http://www2.ohchr.org/english/bodies/cerd/cerds75.htm. See also HRIC's recent parallel reports to UN bodies: Human Rights in China, Implementation of the Convention on the Elimination of All Forms of Racial Discrimination in the People's Republic of China: A Parallel NGO Report by Human Rights in China, June 2009, http://www.hrichina.org/public/PDFs/Reports/2009-CERD—Report.pdf; Human Rights in China, Implementation of the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment in the People's Republic of China: A Parallel NGO Report by Human Rights in China, October 2008, http://hrichina.org/public/PDFs/Submissions/HRIC-CAT-2008-FINAL.pdf; Human Rights in China, Implementation and Protection of Human Rights in the People's Republic of China: A Parallel NGO Report by Human Rights in China, September 2008, http://hrichina.org/public/PDFs/Submissions/2008—HRIC—UPR—Report.pdf (submitted to the UN Human Rights Council in advance of China's 2009 Universal Periodic Review).

[3] For more detailed discussion on the Chinese government's tools for suppressing information access and exchange, see Ronald Deibert, China's Cyberspace Control Strategy: An Overview and Consideration of Issues for Canadian Policy, February 2010, available at http://www.canadianinternationalcouncil.org; James Fallows, "The Connection Has Been Reset," The Atlantic Monthly, March 2008, http://www.theatlantic.com/magazine/archive/2008/03/-ldquothe-connection-has-been-reset-rdquo/6650/; Andrew Lih, "In Brief: Google's China Move," Andrew Lih Blog, posted on March 23, 2010, http://www.andrewlih.com/blog/2010/03/23/in-brief-googles-china-move/; and Rebecca MacKinnon, "China, the Internet and Google," Rconversation Blog, posted on March 23, 2010, http://rconversation.blogs.com/rconversation/2010/03/china-the-internet-and-google.html.

[4] For instance, Article 19 of the Universal Declaration of Human Rights (UDHR) states that "[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers," while under Article 12, "[n]o one shall be sub-

jected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." UDHR, G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948).

[5] Complete English translations of the criminal verdict of the Beijing No. 1 Intermediate People's Court and the decision of the Beijing Municipal High People's Court against Liu Xiaobo have been made available by HRIC in its quarterly publication China Rights Forum, 2010, no. 1, and will soon be made available at http://www.hrichina.org/public/contents/category?cid=1043. In addition, English translations of the six articles by Liu Xiaobo that formed the basis of his criminal conviction have been made available by HRIC in the same issue of China Rights Forum; a complete English translation of Charter 08 has been made available by HRIC at http://www.hrichina.org/public/contents/85717.

[6] For more information on these and other individuals, see HRIC's press releases and statements at http://www.hrichina.org/public/contents/category?cid=1052.

[7] Presently, two factions within the party, known as the Princeling Faction and the Youth League Faction, are engaged in an intense power struggle. The Princeling Faction has currently seized favorable geopolitical and socioeconomic conditions to gain the upper hand. Their representative, Xi Jinping, is preparing to take over the duties of General Secretary of the CPC from Hu Jintao. Meanwhile, Li Keqiang, the representative of the Youth League Faction, is preparing to take over from Wen Jiabao as the Premier of the State Council. However, much can happen between today and the fall of 2012, and what will happen in the end is still uncertain.

[8] Since May 2002, HRIC has submitted 60 individual cases to the WGAD with 17 opinions issued by the WGAD. The conclusion of each and every one of these opinions is that the detention in question is arbitrary, meaning that individuals were being detained for exercising fundamental freedoms or that the circumstances of their detentions violated international standards and norms. The U.S. government should urge action on the part of the Chinese government in these and other cases of arbitrary detention of courageous activists and individuals. By releasing these individuals, China will demonstrate its respect for international human rights and its compliance with the decisions of international human bodies.

[9] See Human Rights in China, "Human Rights: Everyone's Business," China Rights Forum, 2008, no. 1, http://www.hrichina.org/public/contents/category?cid=164873.

PREPARED STATEMENT OF EDWARD BLACK

MARCH 24, 2010

Good afternoon. We appreciate the efforts of this Commission and especially Chairmen Dorgan and Levin to address the issue of Internet freedom, and I thank you for the opportunity to testify today. It is an issue that will impact the shape of the world we will live in, especially with regard to trade, privacy and human rights. For too long the U.S. business community has had insufficient support from the U.S. Government in responding to other nations' efforts to censor or spy on their citizens, and to interfere with the reasonable flow of services, products, and information. Companies are on the front lines in the battle for Internet freedom, but when they are confronted with foreign government demands, the governments that represent these companies must lead in the defense of Internet freedom and free trade principles.

While I now represent a wide variety of technology and communication companies, I was honored to served in the State and Commerce Departments under five Secretaries in the 1970's, and early 80's, where I worked on East-West trade and was actively involved in the approval of the first U.S./China trade agreement. I later chaired and still serve on the State Department's Advisory Committee on International Communication and Information Policy. The interconnection between trade and human rights, including freedom of expression, is an issue I have seen from various vantage points and have cared deeply about throughout my career.

Our nation founded the Internet. Since that time, our government, and those who are committed to freedom and democracy, should have been out there creating and promoting visionary multilateral understandings designed to maximize freedom on the Internet. We are still at an historic crossroads, and we need to seize the opportunity to ensure the Internet lives up to its potential to spread knowledge, awareness, and expand human potential. If we do not lead, we can expect other governments to stifle or distort that potential.

Over the past decade the Internet has grown into the most efficient tool to communicate, exchange information, spark innovation and extend opportunity to many millions around the world. The Internet platform provides a level playing field for anyone to access information, and it gives disadvantaged people and underrepresented and oppressed groups around the world new opportunities to participate in economic, social, cultural and political activity.

Access to the Internet—and the ability to fully use it for communication, commerce, and exchanging information—is more than just a First Amendment issue in this country. The United Nations recognizes freedom of expression as a right. Inter-

net freedom is nothing less than freedom of expression in the 21st century. It must become a top-tier human rights, foreign policy and trade issue.

Freedom and openness are the essence of the Internet, which is what makes it such a powerful communications tool. Totalitarian regimes have depended on tightly controlling the flow of information, both domestically and from the outside world, and they have been increasingly restricting the Internet to maintain their control of information. It is a natural temptation for any government to want to achieve its goals by all means possible. This makes the Internet a tempting target to turn into a tool of state control. But we must protect Internet openness not just from those who want to use it for repression, but also from the many seemingly noble, well-meaning efforts to control specific content or monitor Internet traffic.

Direct challenges to the openness and freedom of the Internet are serious and dangerous. In the long run, though, we may find an equally great threat to Internet freedom will come not from direct attacks, which strike a fatal blow, but from a chipping away of openness—a death by a thousand cuts. This happens as every seemingly well-intentioned effort to remedy a societal problem wins an exception to openness. Repressive regimes use that same technology, and rationale, to filter the Internet or spy for reasons our nation does not support. Our best response to this is for countries who support freedom of expression, non-governmental organizations and consortia like the Global Network Initiative (GNI) to work together to adopt a common ethic of principles for Internet freedom, and to build on that support in whatever form and by whatever means are possible.

My testimony explains that: (a) Internet censorship is a human rights issue and a trade issue; and (b) Internet freedom is a principle that countries purporting to espouse democracy and the welfare of their citizens should practice and protect. Internet freedom must be advanced through leading by example here at home and using negotiations, human rights reports and trade agreements to build international support for Internet freedom principles so as to make outliers of countries that seek to isolate their citizens and use the Internet for censorship, spying and repression.

CENSORSHIP IS A HUMAN RIGHTS ISSUE

The Internet can be the greatest tool in history for people to gather information, communicate and provide a more open, transparent relationship between government and its citizens. Or, the Internet can be among the greatest tools for political repression—depending on how it is used. If we fail to take action, others may pervert the Internet and finally bring about the Orwellian future we thought we had avoided, one in which governments perpetually spy, surveil, censor and control—and say they are doing it for our own good.

We fail the citizens of China, Vietnam, Iran and many other Internet-Restricting Countries when we fail to note their governments' censorship[1] and website blocking in human rights reports. For example, in the 2007 Country Reports on Human Rights issued by the State Department, China was upgraded on its human rights issues—despite the apparent increase that year in censorship and surveillance on the Internet.

To respond to government crackdowns on protesters while looking away when a government cracks down on access to the open Internet sends a signal that we are not serious about Internet freedom. The U.S. Government must consistently treat Internet freedom as a human rights issue in its dealings and communications with foreign governments.

The need for countries that support freedom of expression to use trade and diplomatic means to exert pressure on Internet censorship is only increasing. Every week we fail to take strong action seems to be viewed as a green light by Internet Restricting Countries like China to further curtail Internet freedom. Last month, China announced new trial restrictions on Internet websites. According to the Associated Press, anyone wanting to start a website in China must now submit identity cards, photos of themselves and meet with Chinese regulators and service provides before they can register their website. The Chinese government claims this will reduce pornography, but it will clearly also crack down on anyone disagreeing with the government online.

We're here today partly because of the high profile battle of a major technology company in China. But the number of companies and countries impacted are far

[1] While the policy discussion around Internet-restricting countries often refers to "censorship", there are in fact a variety of practices at issue. When we casually refer to Internet censorship, we must recognize that this includes restrictions such as filtering, blocking, and delaying; state-imposed penalties for posting "wrongthink" online; as well as the self-censorship induced by perpetual state surveillance.

greater. There are few easy answers for companies as they try to bring their technology services and communications tools into nations that have different rules about free speech and freedom of expression. Without the backing of their own government, companies often are faced with the unappealing decision to follow local laws or else exit the market. Staying and engaging can in some cases offer choices to citizens in a repressive country that they wouldn't otherwise have. What companies face varies from country to country. The involvement of the federal government, pushing for a common ethic, can help ease the complexity companies are forced to handle in negotiating operating deals. But the complexity and diversity of situations faced by companies means that rigid statutory solutions may cause unexpected problems and even be counterproductive.

Ultimately countries—not companies—must battle countries on human rights issues. But companies are working alongside government and human rights groups to support Internet freedom. The Global Network Initiative (GNI) is a collaborative project begun in 2008 in which a handful of American companies, including Microsoft, Google and Yahoo!, participate with international human rights organizations and academics to find productive pathways forward in the quest for Internet freedom and unimpeded commercial market access, being careful not to jeopardize employees or other citizens in Internet Restricting Countries. Key Members of Congress, including Senator Richard Durbin (D–IL) and Rep. Chris Smith (R–NJ), have expressed strong support for GNI and Secretary Clinton did so as well in a major policy address in January. Congress and the Administration should encourage broader participation in the GNI by a wider range of U.S. companies, foreign nations and foreign and multinational corporations.

I have seen China make extraordinary strides through economic engagement with the outside world to the point where it is now one of the most influential economies in the world. However, while a policy of engagement may be a necessary condition for increased freedom, it is not in and of itself sufficient to create freedom. As U.S. companies face pressure from the Chinese government in the course of their business activities in China, support from their own government is needed to ensure that they are not taken advantage of, and that China understands that access to its markets is not a coin that enables them to buy their way out of respecting human rights and freedom. Countries that have supported China's growth as a world player in the belief that its economic growth would lead to its becoming a "responsible stakeholder" need to take a stand when China's unreasonable demands on issues like Internet censorship prove inconsistent with such responsibility.

CENSORSHIP IS A TRADE ISSUE

The United States is an information economy, and U.S. companies are leading vendors of information products and services. In this context, information discrimination by other countries fundamentally undermines U.S. economic interests, including the interests of U.S. companies seeking to access foreign markets, including those engaged in electronic commerce. Filtering American content and services has the effect of filtering American competition, and combating it should top our trade agenda.

The development of the Internet has led to a revolution in the way we conduct international commerce and trade. The success of e-commerce depends on users feeling comfortable and secure enough to utilize the services our industry provides. That comfort and security can only exist in an environment of Internet freedom. When a foreign government stifles online freedom or otherwise restricts the Internet, it creates a hostile market environment by preventing its consumers from fully using new products, applications and services offered by or through U.S. tech companies.

Government restrictions on the Internet affect trade in a variety of ways, including as follows:

- Information discrimination represents a classic "non-tariff trade barrier" (NTB) that U.S. trade policy should dismantle. By attempting to co-opt U.S. businesses into content filtering, offenders create barriers to market entry that would not otherwise exist.
- Information discrimination constitutes an unfair "rule of origin" by filtering out (through a nontransparent process) U.S.-originating content such as certain U.S. domains deemed to be "subversive."
- Information discrimination also violates the fundamental free trade principle of "national treatment" to U.S. services and service providers. This provides a leg up to foreign competitors of U.S. companies, thus allowing U.S. companies to be perceived as being coerced into lowering their corporate moral standards and leading to negative public reaction and even penalties at home.

- The WTO requires transparency and access to judicial or administrative review for measures affecting trade in services. Foreign governments, however, regularly restrict the Internet without transparency and accountability.
- When a country blocks access to a U.S. search engine or website, the advertising on those sites is also being blocked, and trade in the products and services advertised are interfered with. This could particularly impact small businesses that rely on U.S. websites to reach international markets.

If foreign governments push U.S. tech companies out of their domestic market, small businesses that rely on these sites to advertise or directly sell goods would be forced to do business instead with those nations' domestic companies that offer similar services that compete with U.S. companies. Indeed, the unreasonable demands the Chinese government has continuously placed on U.S. companies—from censorship coercion to Green Dam to Indigenous Innovation—all seem to have the added objective of clearing the competitive deck of foreign companies.

A special note with respect to China: the Chinese government has been pursuing various "indigenous innovation" policies aimed at controlling technology development and promoting local technology companies. These technology policies extend to the Internet space as well, where Chinese government has been making it difficult for foreign companies to compete and favoring local companies. China's Indigenous Innovation procurement requirement requires Chinese government agencies to purchase only products for which intellectual property was developed and owned in China. Both Indigenous Innovation and Internet censorship are policies that set the price of access to the Chinese market at an unacceptable level of submissiveness.

The European Union was laudably quick to take the first step to recognize and respond to the issue of Internet freedom as a trade issue. In 2007, the European Parliament overwhelmingly passed a proposal to treat Internet censorship as a trade barrier by a vote of 571–38. Hopefully, the European Commission will soon take the necessary further action to implement this policy.

FIRST STEPS TO PROMOTE INTERNET FREEDOM

Having neglected to devote appropriate attention to foreign governments' restrictions of Internet content and services, we now have considerable work before us. This is where we should begin:

- The U.S. Government should investigate cases of Internet censorship and
- The United States Trade Representative (USTR), the State Department and Commerce Department should raise issues of Internet restrictions and combat them using the means of their respective offices. Secretary Clinton's major policy speech is an especially noteworthy and commendable beginning. We appreciate actions like the letter the USTR issued in June after China announced all personal computers sold as of July 1 must have the Green Dam Internet filtering software. But our nation has historically missed opportunities to use our existing trade agreements or even reports as leverage in constraining Internet restrictions, censorship, and surveillance.
- USTR should highlight Internet censorship policies in trade reports. In 2006, the USTR issued a report that was billed as a top to bottom review of U.S.-China trade relations. The report discussed simple infringement of intellectual property, yet did not even mention Internet censorship policies. In U.S. Government trade reports, more attention needs to be paid to Internet restrictions taken in the name of censorship. Every year, the USTR conducts the Special 301 review, in which we assess our trade relationships with an eye toward intellectual property protection. Do principles of free expression deserve any less protection? If we are willing to make adequate protection for copyrighted movies a litmus test for our trade relations, how can Internet freedom be worthy of any less?
- In its annual reports on trade barriers, the USTR should review foreign government restrictions on the Internet—taken in the name of censorship or otherwise—and take appropriate action. If it is found that censorship and surveillance impairs U.S. business interests, we should reassess and adjust our trade relationships accordingly.
- Ultimately, the U.S. Government should negotiate provisions that promote Internet commerce, openness and freedom in trade and other agreements.
- The U.S. Government should use existing trade agreements wherever appropriate to address Internet restrictions.
- The State Department should actively support GNI. It already lends financial support to censorship technology circumvention projects in Internet Restricting Countries. By encouraging broader American corporate responsibility and participation in GNI, and by seeking the participation of our allies abroad

such as the European Union, Congress and the State Department could boost GNI's visibility and effectiveness worldwide.

- The potential effectiveness of treating and contesting Internet censorship as a trade barrier lies in the fact that there is a global rules-based system on trade that nations are obligated to follow. A multilateral rules-based approach may create the necessary leverage to make Internet Restricting Countries respect the economic significance of restricting Internet freedom.

INTERNET FREEDOM BEGINS AT HOME

In addition to using existing trade agreements and human rights monitoring to combat Internet censorship and spying, the United States must lead by example when in comes to Internet freedom and openness by being a model:

We should look at policies enacted by Congress or various government agencies to see if they grow Internet access and increase competition among Internet Access Providers. The competition will help when dealing with another threat to the open Internet—legal or policy changes that allow network level discrimination among end users and messages on the Internet.

We should discourage censorship and surveillance ourselves, restrict intrusive practices such as deep packet inspection and think twice before attempting to block content perceived to be unsavory. Once openness erodes, it's hard to get it back.

We must lead by example. While it is tempting to assume warrantless monitoring of telephone calls, burdensome search engine subpoenas, and regulatory power grabs are not to be equated with the systematic oppression in authoritarian states, these distinctions are hard to make to the rest of the world. To say that our government coerces Internet companies for noble causes while others do so to repress is missing the point: quibbling about the order of magnitude of civilian monitoring will undermine the bold leadership that is necessary to backstop U.S. Internet companies when they are facing down the Thought Police around the world. If our government leads the fight for Internet freedom—by example at home and by negotiations around the world—it will provide invaluable political support to U.S. companies trying to honestly and ethically compete in challenging markets.

CONCLUSION

If the U.S. Government and others who value liberty, do not push Internet freedom to the top of the priority list now, they will be failing the future. We are now faced with a "dangerous opportunity." China's policy of coerced censorship has now become a matter of global public concern. The U.S. Government should take advantage of this moment by pushing for substantive policies that would not only support U.S. businesses resisting Internet oppression, but would also ensure that no company is left to combat a foreign government's Internet repression on its own. If the U.S. Government does not take meaningful action, foreign governments will conclude that they are free to pick off individual companies and intimidate them into submission.

Nations that support human freedom, dignity, and democracy should ensure Internet freedom starts at home and set standards by adopting policies that support a free open Internet. If the Internet is to fulfill its potential as the printing press of the Digital Age, neither a government nor an Internet access provider should act as a gatekeeper, quashing access and content at their whim. At the end of the day, companies can't fight repressive regimes alone on Internet freedom. They need government to lead.

Oppressive foreign governments may not easily change their ways but they need to be made to understand the depth of U.S. and international commitment to Internet openness and freedom. We need to elevate this issue to the top of our diplomatic and trade agenda. Finally, we must be consistent with our own Internet freedom policies and fight for Internet freedom as a common principle so that other nations understand our commitment to curbing censorship of the Internet and threats to Internet freedom in whatever form they manifest.

PREPARED STATEMENT OF MARK PALMER

MARCH 24, 2010

As the father of modern China, Sun Yat-sen once noted: "Worldwide trends are enormous and powerful; those who follow them prosper, and those who resist them perish." The Internet is the most powerful force for progress in our lifetimes. The fact that more than 400 million Chinese already are online testifies to its enormous importance for China.

At a time when Freedom House, the State Department and others have documented increasing censorship of the Internet, and an overall decline of human rights in China and across the globe, it is easy to become pessimistic about the Internet's prospects. But I believe we need to look more deeply at recent history, at what the Chinese people themselves want, at what we can do to respond to their aspirations and at what the State Department for three years has refused to do.

The single most strategic failure of our best minds in the intelligence, journalist and academic communities over the past half century has been their failure to anticipate, indeed even allow for, peaceful democratic revolution. And yet some 60 such revolutions have occurred in countries as divergent as Indonesia, the Philippines, South Africa, Chile, and Ukraine.

We have neither understood what is going on in the minds of elites beneath the closed surface of dictatorships nor the power of students, women and others once they organize. We now know from his secretly tape-recorded, recently published memoir, that Zhao Ziyang, the General Secretary of the Communist Party of China, ultimately concluded that for China's economic success to continue it must be accompanied by a modern political system with a free press, multiple party elections and an independent judiciary. His predecessor as General Secretary of the Communist Party Hu Yaobang was sacked for heading in the same direction.

Over 11,000 of the most influential thinkers in China have signed in their own names Charter 08 which explicitly calls for all human rights to be respected and an "end to the practice of viewing words as crimes."

I emphasize elite thinking because of my own experience over 40 years of living in and working on European communist countries. While we caught glimpses of their views and debates when they were still in power, I participated in President Reagan's first meetings with General Secretary Gorbachev and was close to the last communist leaders of Hungary, we now understand from numerous documents and interviews how deeply troubled senior and mid-level party officials were with their situations and how often just one man at the top or a small group of elders or security officials held back democratic openings. And I have seen with my own eyes the Iron Curtain coming down across Europe—something conventional wisdom thought was impossible.

Beyond elites, in China today it is quite extraordinary how many public protests take place every day and across the country, some 90,000 a year according to official statistics. The support for Google's splendid determination to resist censorship of the Internet speaks volumes about the desire of hundreds of millions to enjoy the same access and rights as their colleagues in Taiwan and across the developed world.

While Hu Jintao boasts about his own use of the Internet, he also has called for it to be "purified" and said "Whether we can cope with the Internet is a matter that affects . . . the stability of the state." By which he means the stability of the one-party state. He is keenly aware that both elite and popular opinion, if allowed free rein on the Internet, will bring about the fall of communist dictatorship.

This fear of the Internet, of his own people and elites, has led Hu Jintao to unleash a truly massive program to control and censor the Internet. What can we do to ensure that the Chinese people circumvent these controls, to bring the Great Firewall down and not only in China but Iran and other increasingly repressive countries as well?

Some of the students who were present on Tiananmen Square during the 1989 massacre came to the United States and earned doctoral degrees in computer sciences from leading American universities. They realized the enormous popularity and potential of the Internet in China and were urged by Chinese still in China to find ways to use their computer engineering skills to combat growing censorship and growing overall violations of human rights.

Beginning in 2000 they have developed a system of software and servers, which over the past decade has grown to be the world's largest circumvention system, providing for roughly 90 percent of anti-censorship traffic in China and worldwide. About a million Chinese and hundreds of thousands of Iranians are frequent users of this system. It works through the distribution of encrypted, secure, free software and by constantly switching IP addresses, up to 10,000 times per hour, on dedicated servers located across the world. They have built and staffed this system with volunteer labor and virtually no financial support from others.

The major limitation on this Global Internet Freedom Consortium's (GIF) ability to serve even much larger numbers of users and to bring down the Firewall altogether is money. They have had to make hard choices between serving a surge in Iranian users last summer and fall and reducing their availability to Chinese users as their servers were crashing. GIF needs to buy many more servers and finally to support full-time staff. Competing with and staying ahead of over 50,000 heavily financed engineers and censors in China requires a dedicated and properly financed

team. We spend $800 million annually on "old media" like VOA and RFA and an additional $1.7 billion on democracy support. Surely we can and should spend $50 to $100 million per year on a system or systems to circumvent Internet censorship and bring down this firewall.

Realizing the enormous success of this Global Internet Freedom Consortium and its potential, a bipartisan group of Senators and Congressmen appropriated $15 million in 2008 to begin to scale up this system and any others which could demonstrate proven ability to circumvent Internet censorship in China, Iran and elsewhere. And in 2010 another $30 million was appropriated.

In my 26 years within the State Department and 20 years outside working on democracy and human rights, I have never been more convinced of the power of any innovation to help those still living in one of the world's 43 remaining dictatorships, half of them Chinese, to liberate themselves.

I also have never been more appalled at the State Department's refusal to do what is so clearly in the national interest of the United States. In flagrant and now repeated violation of Congressional legislation, the State Department has refused to use the appropriated funds to scale up an existing, successful circumvention system. State Department staff-level officials have made a mockery first of Secretary Rice's and now Secretary Clinton's frequently voiced and sincere commitments to help ensure freedom of the Internet.

Let us take just one dimension of American national interest. There is a profoundly false understanding of the Google-China issue—as if Google must lose its China market because it no longer accepts Google.cn censorship. If the United States acts in the manner we seek, and people in China can access Google.com, sell Baidu stock short. And watch Google pick up support from Iran, Syria, and elsewhere. Google's in a fight and a martyred defeat will not help the cause. It too should be pressing the State Department and working with GIF. If it does so, its franchise throughout the world will be enhanced by orders of magnitude for being not merely a wounded victim but the provider of enhanced closed society access to the Internet.

Fortunately key members of Congress are determined that the State Department finally does the right thing. Senators Brownback, Casey, Kaufman, Kyl, and Specter, three Democrats and two Republicans, wrote to Secretary Clinton on January 20, 2010. After expressing concern that the State Department's use of the FY08 funds "did not materially enhance Internet access," they stressed that "the FY10 Consolidated Appropriations Act requires as a matter of law that the Internet Freedom funds be awarded applicants who currently and demonstrably are able to expand Internet access to large numbers of users living in closed societies that have acutely hostile Internet environments. The intent of this language is clear: funds should facilitate immediate and order-of-magnitude scale-ups of proven, field-tested protocols that facilitate access to the Internet by pro-democracy demonstrators in Iran, China, and elsewhere."

To get the State Department's attention, two weeks ago Senator Brownback put a hold on the confirmation of four ambassadorial and assistant secretary nominations. At a press conference on March 18, the Senator citing renewed State Department interest removed these holds. But he stressed "the objective is clear, and delay is the chief ingredient of the problem. The funds must be rapidly dispersed to groups that possess the current capability of immediately opening access to the Internet for millions of new users. One such group is the Global Internet Freedom Consortium, which operates the Freegate circumvention system relied upon by millions around the world. If there are others that can fulfill these criteria, then the State Department should come forward with clear and convincing evidence and we should support those groups as well."

Senator Brownback continued "But we must act now. If we do not achieve a breakthrough in the next week, I will not hesitate to place holds on future State Department nominations for as long as it takes to move the Department away from policies that will keep the firewalls in business for years." Senator Kyl also spoke at the March 18 press conference, affirmed that he shared Senator Brownback's assessment and will join in future holds.

We strongly urge the Congressional-Executive Commission on China also to press the State Department to move promptly to work out an agreed strategy with concerned Members of Congress.

We all agree that it is profoundly in our interest for the Chinese people to have direct and uncensored access to the Internet, that the censorship be circumvented and ultimately defeated. We have it in our power to achieve this goal. Further delay will be an act of moral cowardice and a failure of strategic vision.

PREPARED STATEMENT OF HON. BYRON DORGAN, A U.S. SENATOR FROM NORTH DAKOTA; CHAIRMAN, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

MARCH 24, 2010

The Commission convenes this hearing today to examine China's censorship of the Internet and the challenges it poses both to advocates of free expression and to U.S. companies doing business in China. The recent controversy over Google's operations makes clear that the Chinese government's regulation of the Internet is both a human rights and trade issue.

In the spring of 2000, Congress debated whether to support PNTR for China. Supporters argued that opening China's markets would improve human rights and level the playing field for U.S. companies. The Internet was expected to lead the way, and it has brought some important changes. Today, China has 400 million Internet users, the most in the world. Chinese citizens now have opportunities to shop online, and communicate with one another and the outside world. And, the Chinese government, to its credit, has invested heavily in Internet infrastructure and sought to bridge the digital divide between rich and poor.

Yet, the larger hopes for genuine openness and freedom have gone unrealized. China's Internet users remain subject to the arbitrary dictates of state censorship. More than a dozen agencies are involved in implementing a host of laws, regulations, and other tools to try to keep information and ideas from the Chinese people.

As Rebecca MacKinnon, a leading expert on media and information technology policy in China, has noted:

> China is pioneering a new kind of Internet-age authoritarianism. It is demonstrating how a non-democratic government can stay in power while simultaneously expanding domestic Internet and mobile phone use. . . . Yet on the other hand, as this Commission's 2009 Annual Report clearly outlined, Communist Party control over the bureaucracy and courts has strengthened over the past decade, while the regime's institutional commitments to protect the universal rights and freedoms of all its citizens have weakened.

The government also continues to strengthen controls over the Internet and to harshly punish citizens such as Liu Xiaobo, who use the Internet to advocate for human rights and political reform. I have a list here of political prisoners in China punished in recent years for Internet activities. It was drawn from the Commission's publicly accessible, Political Prisoner Database. I ask that this list be included in the hearing record.

As this list vividly shows, China's censorship practices and control of the Internet have had a terrible impact on human rights advocates. These include ordinary people who promote political freedoms or try to organize on line, or ethnic groups such as Tibetans attempting to share information about ongoing government repression. We also are learning that Internet censorship and regulation in China has serious economic implications for U.S. companies like Go Daddy and many others. China's Internet regulations often run against basic international trade principles of non-discrimination and maintaining a level playing field.

Testifying before the Commission today is a representative from Google, perhaps the most potent Internet company in the world. In mid-December, Google announced that it had "detected a highly sophisticated and targeted attack on its corporate infrastructure originating from China that resulted in the theft of intellectual property from Google." And just this week Google announced that it will stop censoring its Chinese search engine, by rerouting its China searches to its Hong Kong site. The company also said it would also monitor and publicize any attempts at censorship of its Hong Kong site by the Chinese government.

Google's decision is a strong step in favor of freedom of expression and information. It is also a powerful indictment of the Chinese government's insistence on censorship of the Internet.

We asked the Chinese Embassy if they would like to send a representative to appear before us today, and they declined. They did, however, send a statement, and I move now to have that statement included in the hearing record.

The Commission is dedicated to understanding the connections between trade and human rights in China today. For that reason, we have called on five prominent human rights experts and American business leaders to discuss the impact of Internet censorship in China today. I look forward to hearing from the witnesses about possible ways for the U.S. Government, policy makers and businesses to respond to China's regulation of the Internet from both a human rights and trade perspective.

PREPARED STATEMENT OF HON. SANDER LEVIN, A U.S. REPRESENTATIVE FROM MICHIGAN; COCHAIRMAN, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

MARCH 24, 2010

The purpose of this hearing today is to examine the challenges and hazards that the Chinese government's control of the Internet poses both to advocates for free expression and to American companies doing business in China.

Nearly one year ago, in April 2009, the Chinese government published its first National Human Rights Action Plan. In this Action Plan, the Chinese government made specific commitments to the role of the Internet in promoting human rights.

As issued by the Information Office of the State Council, the Action Plan states,

> In the period 2009–2010, along with the dissemination of knowledge of the law among the general public, the state will actively rely on . . . the media, including . . . the Internet, to carry out education in human rights in various forms in a planned way, popularizing and spreading knowledge of the law and human rights. . . .

The Action Plan further states the Chinese government's commitment during 2009–2010 to:

> (m)aking good use of the media, including . . . the Internet, to disseminate the knowledge of human rights among the general public and to making good use of new media, including the Internet, to spread knowledge of human rights . . . .

Finally, and very importantly, according to the Action Plan:

> The state will take effective measures to develop the press and publications industry and ensure that all channels are unblocked to guarantee citizens' right to be heard.

These words could not have been clearer. Human rights and the Internet were linked before the Google controversy, and the Chinese government itself linked them. This only underlines the importance of this hearing, and means that there is considerable and appropriate ground to cover today.

The Universal Declaration of Human Rights provides that all people have the right "to seek, receive and impart information and ideas through any media and regardless of frontiers." And yet, under Chinese policies, laws and regulations, private Internet companies are required to censor or filter content that the Chinese government deems politically unacceptable. These requirements impose limits on internationally recognized rights to free expression.

The Internet can be a great tool for free speech and democratic participation. However, just in the last few months, as this Commission has documented, Chinese authorities have detained, imprisoned or affirmed the sentences of numerous individuals for non-violent expression over the Internet. In so doing, the Chinese government has shown that the Internet may be exploited by authorities as a tool to repress speech and to maintain a closed society.

I would like to call attention to one case in particular, involving the writer and professor Liu Xiaobo. On Christmas Day 2009, a Beijing court sentenced Mr. Liu to 11 years in prison for six essays he published online and for his e-mailing Charter 08, a public document calling for political reform and human rights signed by thousands of Chinese citizens. The court in announcing its decision emphasized Mr. Liu's use of the Internet. Even though Mr. Liu did not advocate violence, the court said he had committed the crime of "inciting subversion." Mr. Liu appealed his case, and on February 11, 2010, his appeal was denied. The facts are unambiguous: Mr. Liu has been detained, tried and punished for exercising internationally recognized rights to free expression and association. China does not wish to be labeled a gross violator of human rights, yet the Chinese government makes its determination to eliminate dissent painfully clear to the world. The trial of Mr. Liu shows us that China once again is at an important crossroads, but seems to be turning in the wrong direction.

The Internet provides new forums for the exchange of ideas. People who use the Internet to access information, to exercise internationally recognized rights to free expression, or to engage in non-violent political speech, must be protected. In its National Human Rights Action Plan, the Chinese government itself threw a spotlight on the relationship between human rights and the Internet. Other nations, including ours, have both the responsibility and a legitimate interest in looking closely at that relationship, as this Commission, with the help of our distinguished panel, does today.

PREPARED STATEMENT OF HON. CHRISTOPHER H. SMITH, A U.S. REPRESENTATIVE FROM NEW JERSEY; RANKING MEMBER, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA

MARCH 24, 2010

Thank you, Mr. Chairman and good afternoon to everybody.

And thank you for calling this hearing on Internet freedom. Reporters Without Borders documents that in China alone, at least 72 people are known to be imprisoned for Internet postings. But the victims of the Chinese government's assault on Internet freedom include the entire Chinese people, denied their right to free expression, denied access to information, and often self-censoring out of fear. Even beyond this, the Chinese government's victims include other peoples, tyrannized by governments with which the Chinese government sells or gives its advice on technologies and techniques of Internet repression—reportedly these include Cuba, Vietnam, Burma, Belarus, and Sri Lanka.

Yet we have seen some positive developments. We have seen that some U.S. IT companies really want to do the right thing. Yahoo! has established much stricter policies governing its interactions with repressive governments, working to keep personally identifying information out of their hands.

Google's transformation has been even more impressive. In 2006, I chaired an eight-hour hearing on The Internet in China: A Tool for Freedom or Suppression? The hearing responded to Yahoo!'s cooperation with Chinese Internet police's tracking down of journalist Shi Tao—who is still serving a 10-year prison term for disclosing state secrets, that is, e-mailing to the United States Chinese government orders not to report on the 15th anniversary of the Tiananmen massacre. Google, Yahoo! and Microsoft, among others, testified at that hearing, which broke the ground on the issue of Internet freedom.

Since 2006 I have been meeting with Google executives, and they've known for some time that the theory that their mere presence in the Chinese market would liberalize China, or at least justify their willingness to censor searches had proven mistaken, and that China was growing more repressive.

Two days ago Google fulfilled its January commitment to stop censoring results on its Chinese search engine. This is a remarkable, and welcomed action, and an important boost of encouragement for millions of Chinese human rights activists and political and religious dissidents. Google's recent actions are a blow against the cynical silence of so many when it comes to the Chinese government's human rights abuses—a blast of honesty and courage and a good example of responsible and principled corporate policy.

Today Go Daddy, the world's largest domain name registrar, announces in its submitted testimony that it has "decided to discontinue offering new .CN domain names at this time" out concern "for the security of the individuals affected by" the Chinese government's new requirements for domain registration.

Go Daddy is the first company to publicly follow Google's example in responding to the Chinese government's censorship of the Internet by partially retreating from the Chinese market. Google fired a shot heard 'round the world, and now a second American company has answered the call to defend the rights of the Chinese people. Go Daddy deserves to be praised for this decision. It is a powerful sign that American IT companies want to do the right thing in repressive countries.

But Go Daddy and Google deserve more than praise for doing the right thing in China—they deserve our government's support. We want to see American IT companies doing the right thing—but we don't want to see them forced to leave China for doing so. Now we see that, however well-intentioned, American IT companies are not powerful enough to stand up to repressive governments. Without U.S. Government support, which my bill, the Global Online Freedom Act would provide, they are inevitably forced to play a role in the repressive government's censorship and surveillance.

The Global Online Freedom Act, the legislation I crafted in 2006 and re-introduced in this Congress, would give American IT companies the U.S.-Government backup they need to negotiate with repressive governments.

Let me describe the bill's key provisions. The bill would establish an Office of Global Internet Freedom in the State Department, which would annually designate "Internet restricting countries"—countries that substantially restrict Internet freedom relating to the peaceful expression of political, religious, or ideological opinion or belief. U.S. IT companies would have to report to the State Department any requirement by a repressive government for filtering or censoring search terms—and the State Department would make the terms and parameters of filtering public knowledge, thus "naming and shaming" the repressive countries.

U.S. IT companies would also have to store personally identifying information outside of Internet-restricting countries, so that the repressive governments wouldn't be able to get their hands on it to track dissidents. U.S. IT companies would have to notify the Attorney General whenever they received a request for personally identifying information from a repressive country—and the Attorney General would have the authority to order the IT companies not to comply, if there was reason to believe the repressive government seeks the information for other than legitimate law-enforcement purposes.

In short: the Global Online Freedom Act would give the IT companies the backup of the U.S. Government. If the Chinese or Iranian government tells them to filter a search term, they can point to the Global Online Freedom Act and say that U.S. law doesn't permit it. If the government's Internet police intercept a human rights activist's e-mail, and demand the company turn over personally identifying information on the account, the company will notify the AG, who can then bring the weight of the U.S. Government into the matter.

I would like to thank Google for re-iterating its support for the Global Online Freedom Act; which it recently did in a support letter which we have here today. And I also want to thank the human rights NGOs which have agreed to issue a joint letter of support for the bill: Reporters Without Borders, Amnesty International, Human Rights Watch, Freedom House, Laogai Research Foundation, Wei Jingsheng Foundation, International Campaign for Tibet, China Aid Association, Uyghur-American Association, Committee to Protect Journalists.

The ability of Google and such highly regarded human rights groups to agree in supporting the Global Online Freedom Act is a strong sign that we should all be able to get behind this bill—the bill has even been introduced, with only slight changes, in the European Parliament.

Select List of Political Prisoners Punished for Online Activity

Provided at the

Congressional-Executive Commission on China

Hearing on

"Google and Internet Control in China: *A Nexus Between Human Rights and Trade?*"

Wednesday, March 24, 2010

Dirksen Senate Office Building, Room 628

Congressional - Executive Commission On China

Sample Record Generated by Forthcoming Enhancement to CECC Political Prisoner Database http://www.cecc.gov

Personal Details

CECC Record Num:	2004-03114	**Ethnic Group:**	Han?
Detention Status:	DET	**Religion:**	
Issue Category:	spch	**Occupation:**	professor, law; PC deputy
Main Name:	Liu Xiaobo	**Affiliation:**	
Chinese Characters (Main Name):	刘晓波	**Residence Province:**	Beijing Shi (prov.)
Alternate Name (Lay or Pen):		**Residence Prefecture:**	(na)
Additional Name(s):		**Residence County:**	(na)
Pinyin Name:	Liu Xiaobo		
Sex:	M		
Age at Detention:			

Imprisonment or Detention Detail

Date of Detention:	2008/12/08
Current Prison:	Beijing (general location)
Sentence Length (Years):	11
Sentence Length (Months):	
Sentence Length (Weeks):	
Sentence Length (Days):	
Province Where Imprisoned (or Detained):	Beijing Shi (prov.)
Prefecture Where Imprisoned (or Detained):	(na)
County Where Imprisoned (or Detained):	(na)

Legal Process

Legal Process:	chg/tri/sent-app	**Formal Arrest Date:**	2009/06/23
Trial Court:	Beijing No. 1 Intermediate People's Court	**Trial Date:**	2009/12/23
Sentence Court:	Beijing No. 1 Intermediate People's Court	**Sentence Date:**	2009/12/25
Appeal Court:	Beijing High People's Court	**Appeal Date:**	2009/12/29
Appeal Ruling Court:	Beijing High People's Court	**Appeal Ruling Date:**	2010/02/11
Charge (Statute):	CL97-art105(2)	**Sent. Ends Per PRC:**	
		Actual Date Released:	

Short Summary

On December 25, 2009, the Beijing No. 1 Intermediate People's Court sentenced prominent intellectual Liu Xiaobo to 11 years in prison for inciting subversion. Liu appealed on December 29 and the Beijing High People's Court denied his appeal on February 11, 2010. Prosecutors said he drafted and organized Charter 08, signed by thousands of Chinese and calling for political reform and protection of human rights. The indictment also cites six essays Liu wrote that were posted on overseas Web sites. The essays were critical of the Chinese Communist Party's rule but did not advocate violence; one specifically called for non-violence. Liu was taken into custody on December 8, 2008, a day before Charter 08 was released. Liu's case has been marred by apparent violations of Chinese legal protections for criminal suspects. He was arrested on June 23, 2009. Previously, Liu was detained in 1989 after the Tiananmen protests and served three years reeducation through labor for his writings in 1996.

Congressional - Executive Commission On China

Sample Record Generated by Forthcoming enhancement to CECC Political Prisoner Database http://www.cecc.gov

Personal Details

CECC Record Num:	2008-00668	**Ethnic Group:**	Han
Detention Status:	DET	**Religion:**	
Issue Category:	assoc/civil/dem/spch		
Main Name:	Guo Quan	**Occupation:**	professor (unspec.)
Chinese Characters (Main Name):	郭泉	**Affiliation:**	China New Democracy Party (CNDP); China Democracy Party (CDP)
Alternate Name (Lay or Pen):		**Residence Province:**	Jiangsu Province
Additional Name(s):		**Residence Prefecture:**	Nanjing Shi (pref.)
Pinyin Name:			
Sex:	M	**Residence County:**	Nanjing Shi Muni. Urb. Area (cty.)
Age at Detention:	40		

Imprisonment or Detention Detail

Date of Detention:	2008/11/13
Current Prison:	Nanjing Prison
Sentence Length (Years):	10
Sentence Length (Months):	
Sentence Length (Weeks):	
Sentence Length (Days):	
Province Where Imprisoned (or Detained):	Jiangsu Province
Prefecture Where Imprisoned (or Detained):	Nanjing Shi (pref.)
County Where Imprisoned (or Detained):	Nanjing Shi Muni. Urb. Area (cty.)

Legal Process

Legal Process:	chg/tri/sent	**Formal Arrest Date:**	2008/12/19
Trial Court:	Suqian Intermediate People's Court	**Trial Date:**	2009/08/07
Sentence Court:	Suqian Intermediate People's Court	**Sentence Date:**	2009/10/16
Appeal Court:	Jiangsu High People's Court	**Appeal Date:**	2009/10/23
Appeal Ruling Court:	Jiangsu High People's Court	**Appeal Ruling Date:**	2009/12/22
Charge (Statute):	CL97-art105(1)	**Sent. Ends Per PRC:**	
		Actual Date Released:	

Short Summary

The Suqian Intermediate People's Court in Jiangsu province on October 16, 2009, sentenced Guo Quan, formerly a university professor and a past member of one of the few "democratic" parties allowed in China, to ten years in prison for "subversion of state power," according to Human Rights in China. The court found that Guo used the Internet to organize an "illegal" political party called the "China New Democracy Party," recruited members for the party, published numerous "reactionary" articles online, called for a seven-day stay-at-home boycott of the government, and sought to "overthrow" the socialist system. Authorities detained Guo on November 13, 2008, arrested him on December 19, and held his trial on August 7, 2009. The Jiangsu High People's Court affirmed the lower court's decision on December 22, 2009, according to Boxun. Guo will reportedly serve his sentence at the Nanjing Prison.

Congressional - Executive Commission On China

Sample Record Generated by Forthcoming Enhancement to CECC Political Prisoner Database http://www.cecc.gov

Personal Details

CECC Record Num:	2004-04053	**Ethnic Group:**	Han
Detention Status:	DET	**Religion:**	
Issue Category:	spch/6489/info	**Occupation:**	
Main Name:	Huang Qi		
Chinese Characters (Main Name):	黄琦	**Affiliation:**	
Alternate Name (Lay or Pen):	Nanbo (pen name)	**Residence Province:**	Sichuan Province
Additional Name(s):		**Residence Prefecture:**	Chengdu Shi (pref.)
Pinyin Name:			
Sex:	M	**Residence County:**	Chengdu Shi Muni. Urb. Area (cty.)
Age at Detention:			

Imprisonment or Detention Detail

Date of Detention:	2008/06/10
Current Prison:	Chuandong Prison
Sentence Length (Years):	3
Sentence Length (Months):	
Sentence Length (Weeks):	
Sentence Length (Days):	
Province Where Imprisoned (or Detained):	Sichuan Province
Prefecture Where Imprisoned (or Detained):	Dazhou Shi (pref.)
County Where Imprisoned (or Detained):	(na)

Legal Process

Legal Process:	chg/tri/sent	**Formal Arrest Date:**	2008/07/18
Trial Court:	Wuhou District People's Court	**Trial Date:**	2009/08/05
Sentence Court:	Wuhou District People's Court	**Sentence Date:**	2009/11/23
Appeal Court:		**Appeal Date:**	
Appeal Ruling Court:	Chengdu Intermediate People's Court	**Appeal Ruling Date:**	2010/02/08
Charge (Statute):		**Sent. Ends Per PRC:**	
		Actual Date Released:	

Short Summary

The Wuhou District People's Court in Chengdu city, Sichuan province, sentenced rights activist Huang Qi on November 23, 2009, to three years in prison for illegal possession of state secrets. The court refused to provide a copy of the verdict and indicated only that the state secrets were city government documents. Huang's lawyer said the documents were publicly available. Huang had visited the Sichuan earthquake zone and wrote about collapsed schools and posted parents' appeals on his human rights Web site. He was detained shortly thereafter on June 10, 2008, and arrested on July 18. The court held his closed trial on August 5. Authorities reportedly kidnapped a person to prevent him from testifying for Huang. Huang suffers from numerous medical conditions, including tumors in his abdomen and hepatitis B, but authorities reportedly have refused to treat him. His appeal was denied on February 8, 2010. He is serving his sentence at the Chuandong Prison in Sichuan.

Congressional - Executive Commission On China

Sample Record Generated by Forthcoming Enhancement to CECC Political Prisoner Database http://www.cecc.gov

Personal Details

CECC Record Num:	2009-00182	**Ethnic Group:**	
Detention Status:	DET	**Religion:**	
Issue Category:	spch/assoc/enviro	**Occupation:**	
Main Name:	Tan Zuoren		
Chinese Characters (Main Name):	谭作人	**Affiliation:**	
Alternate Name (Lay or Pen):		**Residence Province:**	Sichuan Province
Additional Name(s):		**Residence Prefecture:**	Chengdu Shi (pref.)
Pinyin Name:			
Sex:	M	**Residence County:**	(na)
Age at Detention:			

Imprisonment or Detention Detail

Date of Detention:	2009/03/28
Current Prison:	Wenjiang PSB Det. Ctr.
Sentence Length (Years):	
Sentence Length (Months):	
Sentence Length (Weeks):	
Sentence Length (Days):	
Province Where Imprisoned (or Detained):	Sichuan Province
Prefecture Where Imprisoned (or Detained):	Chengdu Shi (pref.)
County Where Imprisoned (or Detained):	Wenjiang Cty.

Legal Process

Legal Process:	chg/tri	**Formal Arrest Date:**	2009/04/24
Trial Court:	Chengdu Intermediate People's Court	**Trial Date:**	2009/08/12
Sentence Court:	Chengdu Intermediate People's Court	**Sentence Date:**	2010/02/09
Appeal Court:		**Appeal Date:**	
Appeal Ruling Court:		**Appeal Ruling Date:**	
Charge (Statute):		**Sent. Ends Per PRC:**	
		Actual Date Released:	

Short Summary

The Chengdu Intermediate People's Court in Sichuan province sentenced writer and environmental activist Tan Zuoren to five years in prison and an additional three years' deprivation of political rights on February 9, 2010, for "inciting subversion of state power." The court reportedly convicted Tan for attempting to organize activities to commemorate the 20th anniversary of the June 1989 Tiananmen protests. The court said Tan posted articles on the Internet about the 20th anniversary and had contact with "hostile foreign forces" such as Tiananmen exile and student leader Wang Dan. Tan had been active in calling for the government to investigate the cause of the large number of school collapses in the May 2008 Sichuan earthquake. He began his own investigation and had published preliminary results before his detention in March 2009. The conduct of his trial on August 12, 2009, reportedly was marred by official abuses and procedural violations.

Congressional - Executive Commission On China

Sample Record Generated by Forthcoming Enhancement to CECC Political Prisoner Database http://www.cecc.gov

Personal Details

CECC Record Num:	2004-05482	**Ethnic Group:**	Han
Detention Status:	DET	**Religion:**	
Issue Category:	spch	**Occupation:**	journalist, newspaper
Main Name:	Shi Tao	**Affiliation:**	
Chinese Characters (Main Name):	师涛	**Residence Province:**	Shanxi Province
Alternate Name (Lay or Pen):		**Residence Prefecture:**	Taiyuan Shi (pref.)
Additional Name(s):	Nice Ears (pen name)	**Residence County:**	(na)
Pinyin Name:			
Sex:	M		
Age at Detention:	36		

Imprisonment or Detention Detail

Date of Detention:	2004/11/24
Current Prison:	Deshan Prison
Sentence Length (Years):	10
Sentence Length (Months):	
Sentence Length (Weeks):	
Sentence Length (Days):	
Province Where Imprisoned (or Detained):	Hunan Province
Prefecture Where Imprisoned (or Detained):	Changde Shi (pref.)
County Where Imprisoned (or Detained):	Wuling Dist.

Legal Process

Legal Process:	chg/tri/sent	**Formal Arrest Date:**	2004/12/14
Trial Court:		**Trial Date:**	2005/03/11
Sentence Court:		**Sentence Date:**	2005/04/27
Appeal Court:	Hunan High People's Court	**Appeal Date:**	
Appeal Ruling Court:	Hunan High People's Court	**Appeal Ruling Date:**	2005/06/02
Charge (Statute):	CL97-art398	**Sent. Ends Per PRC:**	
		Actual Date Released:	

Short Summary

The Changsha Intermediate People's Court in Hunan province sentenced poet and journalist Shi Tao to 10 years' imprisonment on April 27, 2005, for disclosing state secrets to foreigners, a crime under Article 111 of the Criminal Law. The court found that Shi, then editorial director of Contemporary Trade News in Hunan, was informed at an editorial meeting about a secret Communist Party and government order. Reporters Without Borders said the order warned journalists about reporting during the 15th anniversary of the Tiananmen democracy protests. Shi e-mailed his notes about the order to the U.S.-based online newspaper "Democracy Forum." The Hunan High People's Court rejected Shi's appeal on June 2, 2005. Shi's conviction was based in part on evidence provided by Yahoo!'s China office. In November 2007, Yahoo! agreed to pay his family's legal expenses. Shi was detained on November 24, 2004, and arrested on December 14. He is currently serving his sentence in Deshan Prison in Hunan.

Congressional - Executive Commission On China

Sample Record Generated by Forthcoming Enhancement to CECC Political Prisoner Database http://www.cecc.gov

Personal Details

CECC Record Num:	2006-00508	**Ethnic Group:**	Han
Detention Status:	DET	**Religion:**	
Issue Category:	spch	**Occupation:**	writer, poet
Main Name:	Zhang Jianhong	**Affiliation:**	
Chinese Characters (Main Name):	张建红	**Residence Province:**	Zhejiang Province
Alternate Name (Lay or Pen):	Li Hong	**Residence Prefecture:**	Ningbo Shi (pref.)
Additional Name(s):		**Residence County:**	(na)
Pinyin Name:			
Sex:	M		
Age at Detention:	48		

Imprisonment or Detention Detail

Date of Detention:	2006/09/07
Current Prison:	Qiaosi Prison (No. 6 Prison)
Sentence Length (Years):	6
Sentence Length (Months):	
Sentence Length (Weeks):	
Sentence Length (Days):	
Province Where Imprisoned (or Detained):	Zhejiang Province
Prefecture Where Imprisoned (or Detained):	Hangzhou Shi (pref.)
County Where Imprisoned (or Detained):	Yuhang Dist.

Legal Process

Legal Process:	chg/tri/sent-app	**Formal Arrest Date:**	2006/10/12
Trial Court:	Ningbo Intermediate People's Court	**Trial Date:**	2007/01/12
Sentence Court:	Ningbo Intermediate People's Court	**Sentence Date:**	2007/03/19
Appeal Court:		**Appeal Date:**	2007/03/19
Appeal Ruling Court:	Zhejiang High People's Court	**Appeal Ruling Date:**	2007/05/15
Charge (Statute):	CL97-art105(2)	**Sent. Ends Per PRC:**	
		Actual Date Released:	

Short Summary

On March 19, 2007, the Ningbo Intermediate People's Court in Zhejiang province sentenced writer Zhang Jianhong (whose pen name is Li Hong) to six years in prison and one year's deprivation of political rights for "inciting subversion of state power." The court said that in more than 60 articles on overseas Web sites, Zhang had "slandered" China's government and social system. The Zhejiang High People's Court rejected his appeal on May 15. Authorities detained Zhang on September 7, 2006, and arrested him on October 12. Zhang was the founder of the literary and news Web site "Aegean Sea," which authorities shut down in March 2006 for posting news without a license. Zhang reportedly suffers from muscular dystrophy but has not received adequate treatment for months. His wife reported that his condition is steadily deteriorating and that he is unable to walk. Officials have denied Zhang's requests for medical parole. Zhang is currently serving his sentence at the Qiaosi Prison in Zhejiang.

Congressional - Executive Commission On China

Sample Record Generated by Forthcoming Enhancement to CECC Political Prisoner Database http://www.cecc.gov

Personal Details

CECC Record Num:	2008-00545	**Ethnic Group:**	Uyghur
Detention Status:	DET	**Religion:**	Muslim
Issue Category:	eth/spch	**Occupation:**	media, radio
Main Name:	Mehbube Ablesh	**Affiliation:**	
Chinese Characters (Main Name):	阿布露莎	**Residence Province:**	Xinjiang Uyghur Auto. Region
Alternate Name (Lay or Pen):		**Residence Prefecture:**	Wulumuqi [Urumqi] Shi (pref.)
Additional Name(s):		**Residence County:**	(na)
Pinyin Name:			
Sex:	F		
Age at Detention:	29		

Imprisonment or Detention Detail

Date of Detention:	2008/08/dd
Current Prison:	Xinjiang (general location)
Sentence Length (Years):	
Sentence Length (Months):	
Sentence Length (Weeks):	
Sentence Length (Days):	
Province Where Imprisoned (or Detained):	Xinjiang Uyghur Auto. Region
Prefecture Where Imprisoned (or Detained):	(na)
County Where Imprisoned (or Detained):	(na)

Legal Process

Legal Process:	PSB?	**Formal Arrest Date:**	
Trial Court:		**Trial Date:**	
Sentence Court:		**Sentence Date:**	
Appeal Court:		**Appeal Date:**	
Appeal Ruling Court:		**Appeal Ruling Date:**	
Charge (Statute):		**Sent. Ends Per PRC:**	
		Actual Date Released:	

Short Summary

According to Radio Free Asia, Mehbube Ablesh, a Uyghur employee in the advertising department at the Xinjiang People's Radio Station in the Xinjiang Uyghur Autonomous Region (XUAR), was fired from her job in August 2008 and placed in detention, in apparent connection to articles she posted on the Internet that criticized Chinese government policy. According to one source, she had been critical of political leaders in the XUAR and had criticized language policies in the region. Further details about the case, including Mehbube Ablesh's current whereabouts, are not known.

Congressional - Executive Commission On China

Sample Record Generated by Forthcoming Enhancement to CECC Political Prisoner Database http://www.cecc.gov

Personal Details

CECC Record Num:	2009-00080	**Ethnic Group:**	Han?
Detention Status:	DET	**Religion:**	Falun Gong
Issue Category:	FG/rel/spch/info		
Main Name:	Liu Jin	**Occupation:**	librarian
Chinese Characters (Main Name):	刘进	**Affiliation:**	Shanghai Normal University
Alternate Name (Lay or Pen):		**Residence Province:**	Shanghai Shi (prov.)
Additional Name(s):			
Pinyin Name:		**Residence Prefecture:**	Shanghai Shi Muni. Urb. Area (pref.)
Sex:	F	**Residence County:**	Fengxian Dist.
Age at Detention:			

Imprisonment or Detention Detail

Date of Detention:	2007/11/25
Current Prison:	Shanghai Women's Prison
Sentence Length (Years):	3
Sentence Length (Months):	6
Sentence Length (Weeks):	
Sentence Length (Days):	
Province Where Imprisoned (or Detained):	Shanghai Shi (prov.)
Prefecture Where Imprisoned (or Detained):	Shanghai Shi Muni. Urb. Area (pref.)
County Where Imprisoned (or Detained):	Songjiang Dist.

Legal Process

Legal Process:	chg/tri/sent	**Formal Arrest Date:**	
Trial Court:		**Trial Date:**	
Sentence Court:	Fengxian District People's Court	**Sentence Date:**	2008/11/03
Appeal Court:		**Appeal Date:**	
Appeal Ruling Court:		**Appeal Ruling Date:**	
Charge (Statute):	CL97-art300(1)	**Sent. Ends Per PRC:**	
		Actual Date Released:	

Short Summary

According to attorney Mo Shaoping, an AP report, and international Falun Gong organizations, authorities in Shanghai's Fengxian district detained Falun Gong practitioner Liu Jin on the afternoon of November 27, 2007. Police ransacked her home and confiscated personal items including a vehicle and 20,000 yuan. After nearly one year of pretrial detention, the Fengxian District People's Court convicted Liu of "using a cult organization to undermine the implementation of the law" (Criminal Law, Article 300) and sentenced her to 3 years and 6 months in prison on November 14, 2008. The court accused Liu of downloading Falun Gong materials from the Internet and distributing them. Liu served a 4-year sentence from 2001 to 2004 at the Shanghai Women's Prison, where she was reportedly placed in solitary confinement and force-fed. Her husband, Zhang Zhanjie, was imprisoned at Shanghai Tilanqiao Prison from 2001-2005. Liu is being held at the Shanghai Women's Prison, as she was in 2001.

Congressional - Executive Commission On China

Sample Record Generated by Forthcoming Enhancement to CECC Political Prisoner Database http://www.cecc.gov

Personal Details

CECC Record Num:	2009-00128	**Ethnic Group:**	Tibetan
Detention Status:	DET	**Religion:**	Tibetan Buddhist
Issue Category:	eth/info/spch	**Occupation:**	Internet, Web site operator
Main Name:	Konchog Tsephel	**Affiliation:**	Chomei (Web site)
Chinese Characters (Main Name):	贡觉次仁(音)	**Residence Province:**	Gansu Province
Alternate Name (Lay or Pen):		**Residence Prefecture:**	Gannan [Kanlho] Tibetan Auto. Pref.
Additional Name(s):		**Residence County:**	Maqu [Machu] Cty.
Pinyin Name:	Gonjue Cibai		
Sex:	M		
Age at Detention:	39		

Imprisonment or Detention Detail

Date of Detention:	2009/02/26
Current Prison:	Lanzhou (general location)
Sentence Length (Years):	15
Sentence Length (Months):	
Sentence Length (Weeks):	
Sentence Length (Days):	
Province Where Imprisoned (or Detained):	Gansu Province
Prefecture Where Imprisoned (or Detained):	Lanzhou Shi (pref.)
County Where Imprisoned (or Detained):	(na)

Legal Process

Legal Process:	chg/tri-close/sent	**Formal Arrest Date:**	
Trial Court:		**Trial Date:**	
Sentence Court:	Gannan [Kanlho] Intermediate People's Court	**Sentence Date:**	2009/11/12
Appeal Court:		**Appeal Date:**	
Appeal Ruling Court:		**Appeal Ruling Date:**	
Charge (Statute):		**Sent. Ends Per PRC:**	
		Actual Date Released:	

Short Summary

According to a TCHRD report, on February 26, 2009, public security officials detained Konchog Tsephel from his home in Ngulra township, Maqu (Machu) county, Gannan (Kanlho) TAP, Gansu province. Konchog Tsephel operated a Tibetan language Web site (Chomei) featuring Tibetan culture. Officials searched his home, confiscated his computer, and took him to a detention center in Gannan. Konchog Tsephel spent 1989-1994 in India and attended a Tibetan-run school for 3 years. Gansu PSB officials detained him for 2 months in 1995 and subjected him to torture under interrogation. From 1996-1999 he attended university in Beijing and Lanzhou city, Gansu's capital. Konchog Tsephel and a Tibetan poet established the Chomei Web site in 2005; officials shut it down "many times" in 2007-2008, according to TCHRD said. ICT reported that, following a closed trial, the Gannan Intermediate People's Court sentenced Konchog Tsephel on November 12, 2009, to 15 years in prison for disclosing state secrets.

Congressional - Executive Commission On China

Sample Record Generated by Forthcoming Enhancement to CECC Political Prisoner Database http://www.cecc.gov

Personal Details

CECC Record Num:	2009-00206	**Ethnic Group:**	Tibetan
Detention Status:	DET	**Religion:**	Tibetan Buddhist (Gelug)
Issue Category:	eth/rel/spch		
Main Name:	Kunga Tsayang	**Occupation:**	monk, writer
Chinese Characters (Main Name):	贡噶擦尖(音)	**Affiliation:**	Labrang Tashikhyil Mon.
Alternate Name (Lay or Pen):		**Residence Province:**	Gansu Province
Additional Name(s):			
Pinyin Name:	Gongga Cayang	**Residence Prefecture:**	Gannan [Kanlho] Tibetan Auto. Pref.
Sex:	M	**Residence County:**	Xiahe [Sangchu] Cty.
Age at Detention:			

Imprisonment or Detention Detail

Date of Detention:	2009/03/17
Current Prison:	Lanzhou? (general location)
Sentence Length (Years):	5
Sentence Length (Months):	
Sentence Length (Weeks):	
Sentence Length (Days):	
Province Where Imprisoned (or Detained):	Gansu Province
Prefecture Where Imprisoned (or Detained):	Lanzhou Shi (pref.)
County Where Imprisoned (or Detained):	(na)

Legal Process

Legal Process:	chg/tri-close/sent	**Formal Arrest Date:**	
Trial Court:		**Trial Date:**	
Sentence Court:	Gannan [Kanlho] Intermediate People's Court	**Sentence Date:**	2009/11/12
Appeal Court:		**Appeal Date:**	
Appeal Ruling Court:		**Appeal Ruling Date:**	
Charge (Statute):		**Sent. Ends Per PRC:**	
		Actual Date Released:	

Short Summary

According to a March 2009 TCHRD report, on March 17, 2009, public security officials detained monk Kunga Tsayang at his residence in Labrang Tashikhyil Monastery, located in Xiahe (Sangchu) county, Gannan (Kanlho) TAP, Gansu province. Authorities suspected him of writing political essays and posting them on a Tibetan-language Website (Zindri, "Jottings"). Police had monitored Kunga Tsayang for "some time" but he was often away from the monastery traveling. TCHRD described Kunga Tseyang as "a passionate writer, essayist, chronicler, and an amateur photographer" who used the pen name Gangnyi (Son of Snowland). He hailed from Jiuzhi (Chigdril) county, Guoluo (Golog) TAP, Qinghai province, and had traveled in Tibetan and other areas China. The Gannan Intermediate People's Court sentenced Kunga Tsayang in a closed trial on November 12, 2009, to 5 years in prison for "disclosing state secrets," TCHRD reported in November 2009. No information is available about his place of imprisonment.

Statement by Chinese Internet Bureau of the Information Office of the State Council on Google's Withdraw

Foreign companies need to abide by Chinese laws and regulations when they operate in China. Google has violated the written promise it made when entering the Chinese market by stopping filtering its searching service and making thinly-veiled accusation against China. This is totally wrong. We are firmly opposed to the politicization of commercial issues.

On January 12, Google made a public announcement without informing beforehand the Chinese government. It claimed that it was attacked by hackers backed by the Chinese government; it was no longer willing to operate filtered searching services in China and was considering withdrawing from the Chinese market. At the repeated requests from Google, the senior officials of the competent Chinese authorities met with the representatives from Google twice on January 29 and February 25 to hear their opinions. This has fully reflected the sincerity of Chinese side. During the discussions, the Chinese officials responded with great patience and in details to the questions raised by Google. The Chinese side emphasized that China still welcomes Google's operation and development in China provided that it abides by Chinese laws. In the meantime, it is up to Google to decide whether it would withdraw its operation. And if it so decides, it must deal with the follow up work responsibly in accordance with Chinese laws and international norms.

The Chinese government encourages the development and popularization of the internet and is committed to the opening up of the internet. In China, online communications and discussion have become increasingly active and e-business is growing rapidly. What has happened shows that China provides a favorable environment for the development of the internet as well as investment activities. China will continue to pursue the opening up policy, welcome the involvement of foreign companies in the development of China's internet sector and will continue to provide good services for their operation in China. The internet sector in China will maintain a sound momentum for fast development.

PREPARED STATEMENT OF REBECCA MACKINNON, VISITING FELLOW, CENTER FOR INFORMATION TECHNOLOGY POLICY, PRINCETON UNIVERSITY

MARCH 24, 2010

Thank you for the opportunity to submit this testimony for the record. I am Rebecca MacKinnon, a visiting fellow at Princeton University's Center for Technology Policy. From 1992–2001, for more than nine years, I worked as a journalist for CNN in China. For the last six years while based at several different academic institutions I have researched Chinese Internet censorship alongside global censorship trends, examining in particular how the private sector assists government efforts to silence or manipulate citizen speech. I am a founding member of the Global Network Initiative, a non-governmental multi-stakeholder initiative that aims to help Internet and telecommunications companies uphold the principles of free expression and privacy around the world. I am also co-founder of an international bloggers' network called Global Voices Online. Several of our contributors regularly summarize and translate conversations from the Chinese blogosphere, and report on developments related to online free expression in China. My testimony today is informed by my experience as a journalist who has lived under Chinese censorship and surveillance; as a researcher of Chinese Internet censorship; as a practitioner of new media and participant in Chinese-language online communities; and as an advocate for free expression and human rights on the Internet.

On January 12 Google stunned the world with its dramatic announcement that it was reconsidering its business in China in the wake of debilitating cyber-attacks, and furthermore that the company was no longer willing to continue operating a censored search engine in China, Google.cn, launched in January 2006.[1] On March 22, Google redirected Google.cn to the Hong Kong-based search engine Google.com.hk, where it now provides uncensored search results in the simplified character set used by people in Mainland China.[2] In my testimony, I will briefly describe the context of the Google decision. I will then outline some of the different tactics used by the Chinese government to censor and control online speech, including tactics used against Google. I will describe what some Chinese citizens are doing in order to evade and oppose these tactics. Finally, I will offer some specific policy suggestions for how the United States can help to improve Internet freedom in China.

THE CONTEXT OF GOOGLE'S CHINA ANNOUNCEMENT

American Internet company executives have long argued that more connectivity will bring more freedom -even in repressive regimes where the Internet is under heavy censorship and surveillance. Statements to that effect were a common theme in Congressional testimony given by Google and Yahoo executives at the February 2006 hearing convened by the late Rep. Tom Lantos.[3] Since then, Chinese Internet usage has nearly quadrupled. Stories abound of how Internet users in China have helped expose corruption, bring justice to innocent victims of official malfeasance, and even change some laws and regulations. But this has not changed the regime's repressive attitude toward dissent. According to a recent report by the Dui Hua Foundation, in 2008 arrests and indictments on charges of "endangering state security"—the most common charge used in cases of political, religious, or ethnic dissent—more than doubled for the second time in three years.[4]

China is pioneering a new kind of Internet-age authoritarianism. It is demonstrating how a non-democratic government can stay in power while simultaneously expanding domestic Internet and mobile phone use. In China today there is a lot more give-and-take between government and citizens than in the pre-Inter-

[1] A new approach to China, by David Drummond,The Official Google Blog, Jan. 12, 2010, at: http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

[2] A new approach to China: an update, by David Drummond, The Official Google Blog, March 22, 2010 at: http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html

[3] 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, by Elliot Schrage, Vice President, Global Communications and Public Affairs, Google Inc., at: http://googleblog.blogspot.com/2006/02/testimony-internet-in-china.html; and Testimony of Michael Callahan, Senior Vice President and General Counsel, Yahoo! Inc., Before the Subcommittees on Africa, Global Human Rights and International Operations, and Asia and the Pacific, February 15, 2006, at: http://yhoo.client.shareholder.com/press/ReleaseDetail.cfm?ReleaseID=187725

[4] "Chinese State Security Arrests, Indictments Doubled in 2008," Dui Hua Human Rights Journal, March 25, 2009, at: http://www.duihua.org/hrjournal/2009/03/chinese-state-security-arrests.html

net age, and this helps bolster the regime's legitimacy with many Chinese Internet users who feel that they have a new channel for public discourse. Yet on the other hand, as this Commission's 2009 Annual Report clearly outlined, Communist Party control over the bureaucracy and courts has strengthened over the past decade, while the regime's institutional commitments to protect the universal rights and freedoms of all its citizens have weakened.[5]

Google's public complaint about Chinese cyber-attacks and censorship occurred against this backdrop. It reflects a recognition that China's status quo—at least when it comes to censorship, regulation, and manipulation of the Internet—is unlikely to improve any time soon, and may in fact continue to get worse.

OVERVIEW OF CHINESE INTERNET CONTROLS

Chinese government attempts to control online speech began in the late 1990's with a focus on the filtering or "blocking" of Internet content. Today, the government deploys an expanding repertoire of tactics. They include: deletion or removal of content at the source, device and local-level controls, domain name controls, localized disconnection or restriction, self-censorship due to surveillance, cyber-attacks, government "astro-turfing," local government "outreach," and targeted police intimidation.

- **Filtering or "blocking:"** This is the original and best understood form of Internet censorship. Internet users on a particular network are blocked from accessing specific websites. The technical term for this kind of censorship is "filtering." Some congressional proceedings and legislation have also referred to this kind of censorship as "Internet jamming." Filtering can range in scope from a home network, a school network, university network, corporate network, the entire service of a particular commercial Internet Service Provider (ISP), or all Internet connections within a specific country. It is called "filtering" because a network administrator uses special software or hardware to block access to specified web pages by banning access to certain designated domain names, Internet addresses, or any page containing specified keywords or phrases. A wide range of commercial filtering products are developed and marketed here in the United States by U.S. companies for filtering by parents, schools, government departments, businesses, and anybody else who wants to control how their networks are used. All Internet routers—including those manufactured by the U.S. company Cisco Systems—come with the ability to filter because it is necessary for basic cyber-security and blocking universally reviled content like child pornography. However, the same technology can just as easily be used to block political content. According to the Open Net Initiative (ONI), an academic consortium that has been following global Internet filtering since 2002, more than 40 countries now practice Internet filtering to some extent at the national level. However China's Internet filtering system—known to many as "the Great Firewall of China"—is the most sophisticated and extensive in the world.[6] In its 2009 report on Chinese Internet censorship, the ONI described increasingly pervasive and sophisticated filtering tactics. "In fine-tuning this system," the report concluded, "China is also adopting subtler and more fluid controls."[7]
- **Deletion and removal of content:** Filtering is the primary means of censoring content over which the Chinese government has no jurisdiction. When it comes to websites and Internet services over which Chinese authorities do have legal jurisdiction—usually because at least some of the company's operations and computer servers are located in-country—why merely block or filter content when you can delete it from the Internet entirely? In Anglo-European legal parlance, the legal mechanism used to implement such a system is called "intermediary liability." The Chinese government calls it "self-discipline," but it amounts to the same thing, and it is precisely the legal mechanism through which Google's Chinese search engine, Google.cn, was required to censor its search results.[8] All Internet companies operating within Chinese jurisdiction—

[5] 2009 Annual Report, Congressional-Executive Commission on China, at: http://www.cecc.gov/pages/annualRpt/annualRpt09/CECCannRpt2009.pdf

[6] See Access Denied: The Practice and Policy of Global Internet Filtering by Diebert, et.al. (MIT Press, 2008). Updates and new country reports are posted regularly at the Open Net Initiative website at: http://opennet.net

[7] "China" research profile by Stephanie Wang, Open Net Initiative, published on June 15, 2009 at: http://opennet.net/research/profiles/china

[8] See Race To the Bottom: Corporate Complicity in Chinese Internet Censorship by Human Rights Watch (August 2006), at http://www.hrw.org/reports/2006/china0806/. Also "Search Monitor Project: Toward a Measure of Transparency," by Nart Villeneuve, Citizen Lab Occasional

Continued

domestic or foreign—are held liable for everything appearing on their search engines, blogging platforms, and social networking services. They are also legally responsible for everything their users discuss or organize through chat clients and messaging services. In this way, much of the censorship and surveillance work is delegated and outsourced by the government to the private sector—who, if they fail to censor and monitor their users to the government's satisfaction, will lose their business license and be forced to shut down. It is also the mechanism through which China-based companies must monitor and censor the conversations of more than 50 million Chinese bloggers. Politically sensitive postings are deleted or blocked from ever being published. Bloggers who get too influential in the wrong ways can have their accounts shut down and their entire blogs erased. That work is done primarily not by "Internet police" but by employees of Internet companies.[9]

- **Cyber-attacks:** The sophisticated, military-grade cyber-attacks launched against Google were targeted specifically at GMail accounts of human rights activists who are either from China or work on China-related issues. This serves as an important reminder that governments and corporations are not the only victims of cyber-warfare and cyber-espionage. Human rights activists, whistleblowers and dissidents around the world, most of whom lack training or resources to protect themselves, have over the past few years been victim of increasingly aggressive cyber attacks.[10] The effect in some cases is either to bring down overseas dissident websites at critical political moments, or causing frequent outages, putting great strain on the site's operators just to keep it running. Websites run by Chinese exiles, dissidents, and human rights defenders have seen increasingly aggressive attacks over the past few years.[11] In other cases the effect is to compromise activists' internal computer networks and e-mail accounts to the point that it becomes too risky to use the Internet at all for certain kinds of organizing and communications, because the dissidents don't feel confident that any of their digital communications are secure. Journalists who report on human rights issues and academics whose research includes human rights problems have also found themselves under aggressive attack in places like China, exposing their sources and making it much more risky to work on politically sensitive topics. Like the activists, these groups are unprepared and unequipped to deal with cyber-attacks.[12]
- **Device-level and local controls:** In late spring of 2009 the Ministry of Industry and Information Technology (MIIT) mandated that by July 1 of that year all computers sold in China must be pre-installed with a specific software product called "Green Dam—Youth Escort."[13] While the purpose of "Green Dam" was ostensibly for child protection, researchers inside and outside of China quickly uncovered the fact that it not only censored additional political and religious content, it also logged user activity and sent this information back to a central computer server belonging to the software developer's company.[14] The software had other problems which made it easy for U.S. industry to oppose: It contained serious programming flaws which increased the user's vulnerability to cyber-attack. It also violated the intellectual property rights of a U.S. company's filtering product. Faced with uniform opposition from the U.S. computer

---

Paper, No.1, University of Toronto (June 2008) at http://www.citizenlab.org/papers/searchmonitor.pdf

[9] For more details see "China's Censorship 2.0: How companies censor bloggers," by Rebecca MacKinnon, First Monday (February 2006) at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089; and "The Chinese Censorship Foreigners Don't See," by Rebecca MacKinnon, The Wall Street Journal Asia, August 14, 2008, at: http://online.wsj.com/article/SB121865176983837575.html

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

[11] "Chinese human rights sites hit by DDoS attack," by Owen Fletcher, ComputerWorld, January 26, 2010, at: http://www.computerworld.in/articles/chinese-human-rights-sites-hit-ddos-attack

[12] "National Day triggers censorship, cyber attacks in China," Committee to Protect Journalists, September 22, 2009 at: http://cpj.org/2009/09/national-day-triggers-censorship-cyber-attacks-in.php

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

[14] China's Green Dam: The Implications of Government Control Encroaching on the Home PC, Open Net Initiative bulletin (June, 2009) at: http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc; Analysis of the Green Dam Censorware System, by Scott Wolchok, Randy Yao, and J. Alex Halderman, Computer Science and Engineering Division, The University of Michigan, June 11, 2009, at: http://www.cse.umich.edu/%7Ejhalderm/pub/gd/.

industry and strong protests from the U.S. government, the MIIT backed down on the eve of its deadline, making the installation of Green Dam voluntary instead of mandatory.[15] The defeat of Green Dam, however, did not diminish other efforts to control and track Internet user behavior at more localized levels within the national "Great Firewall" system—for instance at the level of a school, university, or apartment block as well as at the level of a city-wide Internet Service Provider (ISP). It was reported in September last year that local governments were mandating the use of censoring and surveillance products with names like "Blue Shield" and "Huadun." The function and purpose of these products appeared similar to Green Dam, though they had the benefit of involving neither the end user nor foreign companies.[16] The implementation of these systems has received little attention outside of China.

- **Domain name controls:** In December, the government-affiliated China Internet Network Information Center (CNNIC) announced that it would no longer allow individuals to register Internet domain names ending in .cn. Only companies or organizations would be able to use the .cn domain.[17] While authorities explained that this measure was aimed at cleaning up pornography, fraud, and spam, a group of Chinese webmasters protested that it also violated individual rights.[18] Authorities announced that more than 130,000 websites had shut down in the cleanup. In January a Chinese newspaper reported that self-employed individuals and freelancers conducting online business had been badly hurt by the measure.[19] Later in February, CNNIC backtracked somewhat, announcing that individuals will once again be allowed to register .cn domains, but all applicants must appear in person to confirm their registration, show a government ID, and submit a photo of themselves with their application.[20] This eliminates the possibility of anonymous domain name registration under .cn and makes it easier for authorities to warn or intimidate website operators when "objectionable" content appears.
- **Localized disconnection and restriction:** In times of crisis when the government wants to ensure that people cannot use the Internet or mobile phones to organize protests, connections are shut down entirely or heavily restricted in specific locations. There have been anecdotal reports of Internet connections going down or text-messaging services suddenly not working in counties or towns immediately after local disturbances broke out. The most extreme case however is Xinjiang province, a traditionally Muslim region bordering Pakistan, Kazakhstan, and Afghanistan in China's far Northwest. After ethnic riots took place in July of last year, the Internet was cut off in the entire province for six months, along with most mobile text messaging and international phone service. Nobody in Xinjiang could send e-mail or access any website—domestic or foreign. Businesspeople had to travel to the bordering province of Gansu just to communicate with customers.[21] Internet access and phone service have now been restored, but with severe limitations on the number of text messages people can send on their mobile phones per day, no access to overseas websites, and even very limited access to domestic Chinese websites. Xinjiang-based Internet users can only access specially watered-down versions of official Chi-

---

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

[16] "China Clamps Down on Internet Ahead of 60th Anniversary," by Owen Fletcher, IDG News Service, September 25, 2009 at: http://www.pcworld.com/article/172627/china—clamps—down—on—internet—ahead—of—60th—annive rsary.html ; and "China: Blue Dam activated," by Oiwan Lam, Global Voices Advocacy, September 13, 2009 at: http://advocacy.globalvoicesonline.org/2009/09/13/china-blue-dam-activated/

[17] "China tightens control on domain name registration," by Zhao Chunzhe, China Daily, December 14, 2009, at: http://www.chinadaily.com.cn/china/2009-12/14/content—9174767.htm

[18] "China: Online protest against CNNIC," by Oiwan Lam, Global Voices Advocacy, December 22, 2009 at: http://advocacy.globalvoicesonline.org/2009/12/22/china-online-protest-against-cnnic/

[19] "China: More than 100 thousand websites shut down," by Oiwan Lam, Global Voices Advocacy, February 3, 2010, at: http://advocacy.globalvoicesonline.org/2010/02/03/china-more-than-100-thousand-websites-shut-down/

[20] "China Further Tightens Rules for Domain Name Owners," by Owen Fletcher, PCWorld, February 23, 2010, at: http://www.pcworld.com/article/190013/china—further—tightens—rules—for—domain—name—owners.html

[21] "What Internet? China region cut off 6 months now," by Cara Anna, Associated Press via Yahoo! News, January 19, 2010, at: http://news.yahoo.com/s/ap/20100119/ap—on—bi—ge/as—china—internet—blackout

nese news and information sites, with many of the functions such as blogging or comments disabled.[22]

- **Self-censorship due to surveillance:** Surveillance of Internet and mobile users is conducted in a variety of ways, contributing to an atmosphere of self-censorship. Surveillance enables authorities to warn and harass Internet users either via electronic communications or in person when individuals are deemed to be taking their online activities too far. Occasional detention, arrest, or imprisonment of select individuals serves as an effective warning to others that they are being watched. Surveillance techniques include:
  - *"Classic" monitoring:* While Chinese surveillance measures are explained by the government to the public as anti-terrorism measures, they are also broadly used to identify, then harass or imprison peaceful critics of the regime. Cybercafes—the cheaper and more popular option for students and less affluent people—are required to monitor users in multiple ways including ID registration upon entry to the cafe or upon login, surveillance cameras, and monitoring software installed on computers. Surveillance in Chinese cybercafes is known to be so extensive that people who are likely to engage in political conversations online avoid doing so in such facilities.
  - *"Law enforcement compliance:"* In a country like China where "crime" is defined broadly to include political dissent, companies with in-country operations and user data stored locally can easily find themselves complicit in the surveillance and jailing of political dissidents. The most notorious example of law enforcement compliance gone badly wrong was when Yahoo's local Beijing staff gave Chinese police account information of journalist Shi Tao, activist Wang Xiaoning, and at least two others engaged in political dissent.[23] There are other examples of how law enforcement compliance by foreign companies has compromised activists. In 2006, Skype partnered with a Chinese company to provide a localized version of its service, then found itself being used by Chinese authorities to track and log politically sensitive chat sessions by users inside China.[24] This happened because Skype delegated law enforcement compliance to its local partner without sufficient attention to how the compliance was being carried out. China's more sophisticated and politically aware Internet users have long assumed that Chinese-branded e-mail and chat services monitor their communications and share them readily with authorities. As news about these incidents involving foreign-branded products spread among Chinese Internet users, however, many no longer feel that they can trust foreign brands either. They feel they have no choice but to minimize the extent to which they use any Internet or mobile service for politically sensitive conversations for fear that anything and everything might be compromised.
- **Pro-active measures: "astro-turfing" and outreach:** The government increasingly combines censorship and surveillance measures with pro-active efforts to steer online conversations in the direction it prefers. In 2008 the Hong Kong-based researcher David Bandurski determined that at least 280,000 people had been hired at various levels of government to work as "online commentators." Known derisively as the "50-cent party," these people are paid to write postings that show their employers in a favorable light in online chat rooms, social networking services, blogs, and comments sections of news websites.[25] Many more people do similar work as volunteers—recruited from among the ranks of retired officials as well as college students in the Communist Youth League who aspire to become Party members. This approach is similar to a tactic known as "astro-turfing" in American parlance, now commonly used by commercial advertising firms, public relations companies, and election campaigns around the world.[26] In many provinces it is now also stand-

[22] "Blogger describes Xinjiang as an 'internet prison,'" Josh Karamay, BBC News, February 3, 2010, at: http://news.bbc.co.uk/2/hi/asia-pacific/8492224.stm

[23] For detailed analysis of the Yahoo! China case see "Shi Tao, Yahoo!, and the lessons for corporate social responsibility," working paper presented at presented December 2007 at the International Conference on Information Technology and Social Responsibility, Chinese University, Hong Kong, at: http://rconversation.blogs.com/YahooShiTaoLessons.pdf

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

[25] "China's Guerilla War for the Web," by David Bandurski, Far Eastern Economic Review, July 2008, at: http://www.feer.com/essays/2008/august/chinas-guerrilla-war-for-the-web

[26] "Astroturfing describes the posting of supposedly independent messages on Internet boards by interested companies and individuals In American politics, the term is used to describe for-

ard practice for government officials—particularly at the city and county level—to work to co-opt and influence independent online writers by throwing special conferences for local bloggers, or inviting them to special press events or news conferences about issues of local concern.[27]

All of these measures are implemented in the context of the Chinese government's broader policies on information and news control. In December the Committee to Protect Journalists listed China as the world's top jailer of journalists.[28]

CITIZEN PUSHBACK

Despite the government's formidable array of control tactics, China's determined, creative, and opinionated Internet users have managed to make the Chinese Internet a lively, fun, and often contentious place.[29] Over the past six years I have been involved with a number of Chinese blogger groups, mailing lists, and social networks. Chinese "netizens"—as they call themselves—are doing a range of things to oppose Internet controls:

- **Informal anti-censorship support networks:** I have attended gatherings of bloggers and journalists in China—with varying degrees of organization or spontaneousness—where participants devoted significant amounts of time to teaching one another how to use circumvention tools to access blocked websites. Informal "teach-ins" on how to access Twitter are especially popular among people who want access to an uncensored, international community of conversation. Certain bloggers are known to post information about how to circumvent censorship and welcome their friends to copy and re-post their work as widely as possible. I have seen numerous Powerpoints presentations and PDF documents containing instruction manuals on how to use various tools, circulated by e-mail or through peer-to-peer instant messaging clients.
- **Distributed web-hosting assistance networks:** I am aware of people who have strong English language and technical skills, as well as overseas credit cards, who are helping friends and acquaintances in China to purchase inexpensive space on overseas web hosting services, then set up independent blogs using free open-source software. The objective is to help people who don't have the technical skills to run a website on their own to avoid (a) being victim of content removal if they use domestic services, or (b) being blocked if they use popular international blogging platforms like Blogspot, Typepad, Livejournal, or Wordpress.com, all of which are blocked in China. Sometimes the people doing this largely volunteer work also help bloggers to switch domain names and IP addresses when the blog gains attention and gets blocked by the "great firewall."
- **Crowdsourced "opposition research:"** With the Chinese government's Green Dam censorware edict last year, we have seen the emergence of loosely organized "opposition research" networks. Last June a group of Chinese computer programmers and bloggers collectively wrote a report exposing Green Dam's political and religious censorship, along with many of its security flaws. They posted the document at Wikileaks.[30] Another anonymous group of Chinese netizens have collected a list of companies and organizations—domestic and foreign—who have helped build China's Internet censorship system.[31]
- **Preservation and relay of censored content:** I have noticed a number of people around the Chinese blogosphere and in chatrooms who make a regular habit of immediately downloading interesting articles, pictures, and videos which they think have a chance of being blocked or removed. They then re-post

---

mal public relations projects which deliberately give the impression that they are spontaneous and populist reactions. The term comes from AstroTurf—the fake grass used in many indoor American football stadiums. The contrast between truly spontaneous or "grassroots" efforts and an orchestrated public relations campaign, is much like the distinction between real grass and AstroTurf." From http://www.answers.com/topic/astroturfing

[27] "How China polices the internet," by Kathrin Hille, Financial Times, July 17, 2009 at: http://www.ft.com/cms/s/2/e716cfc6-71a1-11de-a821-00144feabdc0.html

[28] "2009 Prison Census," Committee to Protect Journalists, (as of December 1, 2009) at: http://cpj.org/imprisoned/2009.php

[29] For an excellent portrayal of Chinese Internet culture and its contentious, playful nature see The Power of the Internet in China: Citizen Activism Online by Guobin Yang, (Columbia University Press, 2009).

[30] "A technical analysis of the Chinese "Green Dam Youth Escort" censorship software," posted June 2009 on Wikileaks.org at: http://wikileaks.org/wiki/A—technical—analysis—of—the—Chinese—%27Green—Dam—Youth-Escort%27—censorship—software (At time of writing the page cannot be reached due to bandwith and funding problems at Wikileaks.org)

[32] "A Dirty Pun Tweaks China's Online Censors," by Michael Wines, The New York Times, March 11, 2009, at: http://www.nytimes.com/2009/03/12/world/asia/12beast.html

these materials in a variety of places, and relay them to friends through social networks and e-mail lists.

- **Humorous "viral" protests:** In 2009, Internet censorship tightened considerably. Many lively blogging platforms and social networks where heated political discussions were known to take place were shut down under the guise of an anti-porn crackdown. In response, an anonymous Shanghai-based jokester created an online music video called "Ode to the Grass Mud Horse"—whose technically innocent lyrics, sung by a children's chorus over video of alpaca sheep, contained a string of highly obscene homonyms. The video spawned an entire genre of anti-censorship jokes and videos involving mythical animals whose names sound similar to official slogans and obscenities of various kinds.[32] This viral pranksterism created an outlet for people to vent about censorship, poke fun at the government, and raise awareness among many people who are not comfortable discussing such matters in a direct way.
- **Public persuasion efforts:** A number of prominent liberal Chinese intellectuals and journalists occasionally write essays on personal blogs in which they criticize the government's censorship and information control policies as counterproductive: censorship, they argue, stifles the Chinese people's innovation and creativity, contributes to corruption and economic inefficiency, and generally prevents the nation from fulfilling its real potential. Such arguments have failed to influence government policies in any kind of meaningful way, although individual officials and business leaders sometimes do echo these sentiments in public fora.[33] It remains unclear when or whether this line of argument will eventually convince China's leadership to relax information controls. The good news, however, is that in China today it is at least possible to make this argument.

RECOMMENDATIONS

Because the Chinese government deploys an expanding range of tactics to control online speech, efforts to promote Internet freedom in China should be similarly multi-pronged and multi-faceted. China's Internet users are pushing back against the controls in a range of ways, as I have described. It is thus important to support, encourage, and enable a range of efforts aimed at tackling different parts of the problem. Finally, corporate social responsibility is essential: It will be much more difficult for Chinese Internet users to fight for their rights if the international business community assists the Chinese government in finding more effective means to muzzle them.

- **Anti-censorship tools:** Congress is to be commended for giving both moral and financial support to programmers who are working hard to develop anti-censorship technologies. In spite of this, I have never ceased to be amazed by the number of university students, academics, journalists, and other white-collar professionals I've encountered on frequent trips to China over the past few years who profess little or no knowledge of circumvention tools and techniques. While no survey data exists to shed light on what percentage of Chinese Internet users know how to circumvent censorship—or are interested in doing so even if they know how—the anecdotal evidence I have gathered leads me to concluded that the percentage must be relatively small, and concentrated among elite groups of tech-savvy people who work in the Internet industry, followers of banned religious groups, and politically active people. The broader Internet-using public in China appears to be largely in the dark about how to access blocked websites. Funding for software development, therefore, needs to be accompanied by equally robust support for education and outreach among broader segments of Chinese society beyond the obvious communities.
- **Anonymity and security tools:** In my interactions with Chinese journalists, human rights, lawyers, bloggers, and academics, I've found that most of them are shockingly uneducated about how to evade online surveillance, how to secure their e-mail, how to detect and eliminate spyware on their computers, and how to guard against even the most elementary cyber-attacks. Chinese-language, culturally appropriate technologies, accompanied by robust education and training, is badly needed. The recent attacks against Chinese GMail users only highlights the urgency.

---

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

[33] "Charles Zhang: Without Reform There is No Way Out" by Xiao Qiang, China Digital Times, February 4, 2010, at: http://chinadigitaltimes.net/2010/02/charles-zhang-%E5%BC%A0%E6%9C%9D%E9%98%B3%EF%BC%9Awithout-reform-there-is-no-way-out/

- **Capture, preservation, and distribution of censored content:** As I mentioned earlier, a lot of Chinese Internet users are downloading and preserving content before it gets censored, but in an ad-hoc and unorganized way. A searchable, accessible, and secure repository of such materials would be invaluable if somebody had the time, funds, and technical support to create one.
- **Support for "opposition research":** To date, ad-hoc groups conducting research aimed at exposing details of Chinese censorship policies rely primarily on two platforms to publish their findings: Google Documents and Wikileaks.org. It is unclear whether Google Documents will remain accessible in China if Google shuts down Google.cn and reduces or closes its China operations. Wikileaks.org faces bandwith problems and financial difficulties resulting in frequent inaccessibility. Chinese opposition researchers could use help in finding secure, reliable, and accessible platforms through which their work can be disseminated.
- **Corporate responsibility:** To ensure that American Internet businesses in China assume the appropriate level of responsibility for the human rights of their users and customers, I support a voluntary component backed up by legislation if necessary.
  - Global Network Initiative: In 2008 Google, Yahoo, and Microsoft took the important step of joining the Global Network Initiative (GNI), a code of conduct for free expression and privacy for companies in the Information & Communications Technologies (ICT) sector.[34] The GNI can help companies uphold a shared commitment to the values of free expression and privacy while recognizing that no market is without political difficulties or ethical dilemmas. Just as companies have a social responsibility not to pollute the environment or exploit twelve-year-olds, American companies have a responsibility not to collaborate with the suppression of peaceful speech. The GNI's philosophy is grounded in the belief that people in all markets stand to benefit from Internet and mobile technologies. In most cases companies can still do a lot of good by being engaged in countries whose governments practice at least one of the forms of Internet controls I have described above—as long as they are aware of the human rights implications of their business and technical decisions. It is reasonable to expect all Internet and telecommunications companies to include human rights risk assessments in their decisions about market entry and product development, just as they and other companies consider environmental risks and labor concerns. With a multi-stakeholder membership including human rights groups, socially responsible investors and academics like myself, GNI's goal is to help companies do the right thing while bringing expanded Internet communications and mobile access to the people who stand to benefit from this connectivity the most.

    The principles' implementation guidelines and accountability framework can be adapted to a range of business models, including hardware companies and Internet service providers if these companies choose to engage with the GNI. As this Commission is aware, Senator Dick Durbin has written to 30 companies urging them to join the GNI and we look forward to working with them so that it will be possible for them to join in the near future. While GNI is presently most relevant to Yahoo, Google and Microsoft because those were the three companies that launched the initiative, it is also apparent that the 30 companies contacted by Senator Durbin share varying degrees of human rights risk, even as their business models, technologies, and geographies vary widely. They have an obligation to at least consider joining the GNI and if they choose not to, to find other appropriate policy and operational responses to address the inescapable human rights implications of their products or services.
  - *Legislation:* While recognizing that no connectivity at all is even worse than censored connectivity, and also recognizing that many information communications technologies have "dual use" capabilities that can be used for security and legitimate law enforcement as well as repression, it should nonetheless be made more difficult for U.S. companies to provide censorship and surveillance capabilities to Chinese government entities and their corporate affiliates, given the regime's clear track record of using those technologies to suppress peaceful political dissent. It is important, however, that legislation be flexible enough to accommodate the rapidly changing nature of information communications technology, as well as the complex and

[34] See http://globalnetworkinitiative.org

highly diverse nature of ICT businesses—including many small startups, as well as innovations that are difficult to define, categorize, or predict in advance. It is also important that any law concerning the human rights implications of ICTs be truly global in scope, recognizing that ICT companies can face human rights dilemmas in almost every market, whether the government involved is technically categorized as "democratic" or "authoritarian."

○ *Legal support for victims:* Companies will have a further disincentive to collaborate with repressive surveillance and censorship if victims or corporate collaboration in human rights abuses can more easily sue them in a United States court of law.

○ *Incentives for socially responsible innovation:* Companies should be encouraged to develop technologies and service features that enhance users' ability to evade censorship and surveillance, and to help users better understand what personal information is being stored and how it is used.

CONCLUSION

Many of China's nearly 400 million Internet users are engaged in passionate debates about their communities' problems, public policy concerns, and their nation's future. Unfortunately these public discussions are skewed, blinkered, and manipulated—thanks to political censorship and surveillance. The Chinese people are proud of their nation's achievements and generally reject critiques by outsiders even if they agree with some of them. A democratic alternative to China's Internet-age authoritarianism will only be viable if it is conceived and built by the Chinese people from within. In helping Chinese "netizens" conduct an un-manipulated and uncensored discourse about their future, the United States will not imposing its will on the Chinese people, but rather helping the Chinese people to take ownership over their own future.

QUESTIONS AND ANSWERS SUBMITTED FOR THE RECORD

RESPONSE FROM CHRISTINE JONES TO A QUESTION FROM REPRESENTATIVE DAVID WU

Question. What are one, two, or three things the Federal Government can do to assist you in your capacity?

Answer. To date, China has not enforced significant penalties against spammers and others who utilize the Internet to engage in criminal activities; thus, it has become a sort of safe harbor for such criminals.

Go Daddy's efforts to persuade authorities there to investigate or prosecute spammers have been ineffective, as have our efforts to work with Chinese-based hosting companies to shut down compromised websites.

We hope that the U.S. Government can use its influence with authorities in China to increase Chinese enforcement activities relating to Internet abuse, while encouraging the free exchange of ideas, information, and trade. Specifically, U.S. diplomacy with China should include efforts to effect the retraction of China's recent policies relating to the registration of .CN domain names, which will act as a barrier to Internet access by Chinese nationals.

RESPONSE FROM CHRISTINE JONES TO A QUESTION FROM REPRESENTATIVE MICHAEL HONDA

Question. How does the Chinese government perceive the role or purpose of the Internet? Is it a resource for information or economic benefit? One of the government's main driving forces is stability through economic growth. How do we help Chinese officials to understand the economic benefits through Internet freedom—so that they are encouraged to change their philosophy on censorship and lift their filters? Are there confidence-building steps that our government can make with Chinese officials to instill trust.

Answer. There appears to be a recent increase in China's surveillance and monitoring of the Internet activities of its citizens. In particular, limitations on Chinese nationals ability to register domain names through non-Chinese registrars, and new reporting and verification requirements for .CN registrations appear, to us, to be based on a desire by the Chinese authorities to exercise increased control over the subject matter of domain name registrations by Chinese nationals. In addition, China has not taken adequate steps to prevent spam, cyber-crimes, and other malicious online activity.

By limiting the ability of its citizens to fully engage in the Internet and the free flow of information and the economic productivity it enables, the Chinese government is limiting the economic growth potential of its population. In its trade and

diplomatic meetings with the Chinese government, the United States should encourage the enforcement of internationally recognized norms on law enforcement related to malicious online activity nd seek to have China lift its implicit and explicit limits on domain registrations.

RESPONSE FROM SHARON HOM TO A QUESTION FROM REPRESENTATIVES CHRISTOPHER SMITH AND MICHAEL HONDA

Question. As a member of the United Nations' Human Rights Council, should the United States government call for a hearing in the Human Rights Council on China's human rights practices and censorship of the Internet?

Answer. The U.S. Government needs to demonstrate stronger leadership and more active participation in existing human rights bodies and processes, including the Human Rights Council. There have already been a number of assessments of China's human rights record by various UN human rights bodies that raise concerns regarding Internet censorship, access to information, and protection of freedom of expression and privacy rights. Unfortunately, during the Human Rights Council's Universal Periodic Review of China's overall human rights record in February 2009, the U.S. Government—an observer state—remained completely silent.[1]

Other UN human rights mechanisms available are limited by their specific relevant mandates and are often further weakened by the council's politicized process. Nonetheless, the U.S. Government can still do much more to strengthen the credibility and effectiveness of the work of the Human Rights Council.

The U.S. Government should also actively promote greater protections for online freedom of expression and protection of privacy through greater participation in other international forums, and strategic cooperation with European and other bilateral partners to integrate human rights issues and concerns throughout its trade, human rights, and security policy approaches.

RESPONSE FROM SHARON HOM TO A QUESTION FROM REPRESENTATIVE DAVID WU

Question. What are one, two, or three things the Federal Government can do to assist you in your capacity?

Answer. U.S. leadership on global norm building: In fulfilling its commitment to development of and respect for international law, the U.S. Government must actively participate in the process of developing a global consensus on defining and promoting Internet rights and freedoms within an international human rights framework.

Support for and consultation with civil society: The U.S. Government can also support civil society groups, both in the United States and abroad, including those engaged in important Internet advocacy in restrictive regimes like China. This should include regular consultations with human rights groups, technology developers, information and communications technology (ICT) companies, socially responsible investors, policy think tanks, and academic communities.

Encourage pro-active private sector initiatives: The U.S. Government should continue to encourage individual companies, and business and trade associations, to address and promote more effective approaches to advancing human rights, including freedom of expression and privacy rights. This encouragement should include support for and pressure on ICT companies to participate in multi-stakeholder initiatives, such as the Global Network Initiative.[2]

RESPONSES FROM SHARON HOM TO QUESTIONS FROM REPRESENTATIVE MICHAEL HONDA

Question 1. How does the Chinese government perceive the role or purpose of the Internet? Is it a resource for information or economic benefit? One of the government's main driving forces is stability through economic growth. How do we help Chinese officials to understand the economic benefits through Internet freedom—so that they are encouraged to change their philosophy on censorship and lift their fil-

[1] For more information on the Human Rights Council's Universal Periodic Review of China in 2009, including a summary of all recommendations made by observer states to the Chinese government for greater human rights protections, see Human Rights in China's press releases, including "China's UN Human Rights Review: New Process, Old Politics, Weak Implementation Prospects," February 9, 2009, http://www.hrichina.org/public/contents/127014 and "China Rejects UN Recommendations for Substantive Reform to Advance Human Rights," February 11, 2009, http://www.hrichina.org/public/contents/128130. Recommendations from the U.S. Government are notably absent from the international community's calls for greater human rights reform.

[2] The Global Network Initiative (GNI) is a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics committed to developing a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector. For more information, see http://www.globalnetworkinitiative.org.

ters? Are there confidence-building steps that our government can make with Chinese officials to instill trust?

Answer. The Chinese government's perception of the role and purpose of the Internet has changed over the past decade. As part of its efforts to modernize and deploy high technology, China built its Internet infrastructure via the so-called "Golden Shield Project" to enhance and increase its information control and surveillance capability—largely with the help of foreign ICT companies.[3]

However, the current evolution and rapid growth of the Internet has exceeded the Chinese leadership's initial understanding of its capability to control it. They did not foresee that one day the Internet might provide direct online platforms for public opinion, debate, and broadcast beyond official media for now over 384 million netizens, including 233 million mobile Internet users, and over 50 million bloggers.[4]

The Chinese government also understands very well the economic benefits of the Internet, but the number one policy imperative is to maintain social and political control through Chinese law, a pervasive police and security apparatus, and state-of-the art surveillance and monitoring technology, all of which contribute to self-censorship. Despite this powerful censorship and surveillance capacity, the Chinese government perceives the Internet to pose serious risks to one-party rule.

Therefore, the key challenge is not building confidence, because the Chinese authorities can never be reassured about their greatest fear: loss of power. To ask the Chinese authorities to "change its philosophy on censorship and lift their filters" is like asking a tiger for its skin. However, there are reform forces within Chinese society that desperately need support, encouragement, and confidence-building measures to enhance their own efforts to advance a more open and democratic society in China.

Question 2. Over the years, we have seen Chinese regulations and laws adopted that improve human rights and rule of law standards. However, transparency and enforcement of these have been questionable and lacking. Much of that is due to the lack of oversight on local officials to enforce these rules. In this case, Internet censorship is more of a centralized effort and governance. As Ambassador Palmer stated, one person or small group at the top of the leadership can hold back reforms. I see Internet censorship as a perfect case in point. Do you see the new and upcoming party leaders as more receptive to Internet policy reforms?

Answer. Although there is a widely recognized gap between Chinese law as written on the books and as actually enforced, the one key policy obstacle to greater rights protection is the Chinese leadership's emphasis on "*yifazhiguo*"—to rule the country by law. That is, the key role of Chinese law is to uphold the authoritarian regime. This role is not to be confused with an independent rule *of* law, or "*fazhi.*"

After the 18th National People's Congress in 2012, there will be new faces within the Chinese leadership. Clearly, some are already lining up in the wings. However, no matter who the new leaders are, they will always act in furtherance of the Communist Party of China's special interests. Although they may be receptive to some Internet policy reforms, they will not support any reforms that undermine their hold on power.

Question 3. There are over 400,000 Chinese Internet users. What is the general Chinese public's opinion of the Internet? We have seen a tremendous increase in the number of protests in China, such as ones against poor work conditions and local government corruption. Internet censorship, however, is less visible and tangible. Can we expect a larger popular protest on Internet censorship in China?

---

[3] Multinational corporations deeply involved in creating China's Internet infrastructure include Nortel Networks, Sun Microsystems, and Cisco. See Greg Walton, China's Golden Shield (Montreal: International Centre for Human Rights and Democratic Development, 2001), available at http://www.ichrdd.ca/site/—PDF/publications/globalization/CGS—ENG.PDF.

[4] See China Internet Network Information Center, 25th Statistical Survey Report on Internet Development in China (Beijing: China Internet Network Information Center, 2010), available at http://www.cnnic.cn/uploadfiles/pdf/2010/3/15/142705.pdf.

Answer. The Internet has become an integral part of the daily life of a certain demographic of Chinese people—typically educated, professional, high-income males under the age of 30.[5] However, together with the rapid expansion of mobile technology, social networking tools like Twitter, QQ, and Skype, and the explosive growth of multimedia applications, the Internet has also provided the platform for immediate broadcast of protest footage, documentation of security and police actions, and social mobilization. This empowering role of technology has the further effect of encouraging other citizens to use these tools—all deployed with great spirit and even satirical humor.

[5] Ibid.