AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PROMOTING GLOBAL INTERNET FREEDOM

HEARING

BEFORE THE

SUBCOMMITTEE ON AFRICA, GLOBAL HEALTH, AND HUMAN RIGHTS

OF THE

COMMITTEE ON FOREIGN AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

DECEMBER 8, 2011

Serial No. 112–114

Printed for the use of the Committee on Foreign Affairs

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

U.S. GOVERNMENT PRINTING OFFICE

71–621PDF WASHINGTON : 2011

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

COMMITTEE ON FOREIGN AFFAIRS

ILEANA ROS-LEHTINEN, Florida, *Chairman*

CHRISTOPHER H. SMITH, New Jersey
DAN BURTON, Indiana
ELTON GALLEGLY, California
DANA ROHRABACHER, California
DONALD A. MANZULLO, Illinois
EDWARD R. ROYCE, California
STEVE CHABOT, Ohio
RON PAUL, Texas
MIKE PENCE, Indiana
JOE WILSON, South Carolina
CONNIE MACK, Florida
JEFF FORTENBERRY, Nebraska
MICHAEL T. MCCAUL, Texas
TED POE, Texas
GUS M. BILIRAKIS, Florida
JEAN SCHMIDT, Ohio
BILL JOHNSON, Ohio
DAVID RIVERA, Florida
MIKE KELLY, Pennsylvania
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
JEFF DUNCAN, South Carolina
ANN MARIE BUERKLE, New York
RENEE ELLMERS, North Carolina
ROBERT TURNER, New York

HOWARD L. BERMAN, California
GARY L. ACKERMAN, New York
ENI F.H. FALEOMAVAEGA, American Samoa
DONALD M. PAYNE, New Jersey
BRAD SHERMAN, California
ELIOT L. ENGEL, New York
GREGORY W. MEEKS, New York
RUSS CARNAHAN, Missouri
ALBIO SIRES, New Jersey
GERALD E. CONNOLLY, Virginia
THEODORE E. DEUTCH, Florida
DENNIS CARDOZA, California
BEN CHANDLER, Kentucky
BRIAN HIGGINS, New York
ALLYSON SCHWARTZ, Pennsylvania
CHRISTOPHER S. MURPHY, Connecticut
FREDERICA WILSON, Florida
KAREN BASS, California
WILLIAM KEATING, Massachusetts
DAVID CICILLINE, Rhode Island

YLEEM D.S. POBLETE, *Staff Director*
RICHARD J. KESSLER, *Democratic Staff Director*

SUBCOMMITTEE ON AFRICA, GLOBAL HEALTH, AND HUMAN RIGHTS

CHRISTOPHER H. SMITH, New Jersey, *Chairman*

JEFF FORTENBERRY, Nebraska
TOM MARINO, Pennsylvania
ANN MARIE BUERKLE, New York
ROBERT TURNER, New York

DONALD M. PAYNE, New Jersey
KAREN BASS, California
RUSS CARNAHAN, Missouri

CONTENTS

Page

WITNESSES

Daniel Calingaert, Ph.D., vice president, Freedom House 6
Ms. Clothilde Le Coz, Washington director, Reporters Without Borders 17
Ms. Elisa Massimino, president and chief executive officer, Human Rights First 27
Ms. Rebecca MacKinnon, Bernard L. Schwartz fellow, The New America Foundation 41

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Daniel Calingaert, Ph.D.: Prepared statement 9
Ms. Clothilde Le Coz: Prepared statement 19
Ms. Elisa Massimino: Prepared statement 31
Ms. Rebecca MacKinnon: Prepared statement 43

APPENDIX

Hearing notice 74
Hearing minutes 75
The Honorable Russ Carnahan, a Representative in Congress from the State of Missouri: Prepared statement 76
Written responses received from Freedom House to questions submitted for the record by the Honorable Russ Carnahan 77
Daniel Calingaert, Ph.D.: Exerpt from report submitted for the record 81

PROMOTING GLOBAL INTERNET FREEDOM

THURSDAY, DECEMBER 8, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON AFRICA, GLOBAL HEALTH,
AND HUMAN RIGHTS
COMMITTEE ON FOREIGN AFFAIRS,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:45 p.m., in room 2172, Rayburn House Office Building, Hon. Christopher H. Smith (chairman of the subcommittee) presiding.

Mr. SMITH. The subcommittee will come to order. I want to, first of all, express my apologies to our witnesses and all interested parties for the delay. We did have a series of votes that precluded gaveling this to order at the proper time of 2:00, so I ask for your forbearance.

Good afternoon and welcome to this hearing on global online freedom. About 2 billion people in the world regularly communicate or get information on the Internet. Well over half a billion people do so in repressive countries. As Internet use has become vital and even the standard means to disseminate beliefs, ideas, and opinions, so we see a growing number of countries that censor or conduct surveillance on the Internet in conflict with internationally recognized human rights, laws, and standards.

In 2006, I held the first major hearing ever on Internet freedom, right here in this room in response to Yahoo! turning over the personally identifying information of its email account holder Shi Tao to the Chinese Government, who tracked him down and sentenced him to 10 years for sending abroad emails that revealed the details of Chinese Government press controls. At that hearing Yahoo!, Google, Microsoft, and Cisco testified on what we might ruefully call their worst practices of cooperation with the Internet police of totalitarian governments like China's.

That same week, I introduced the first Global Online Freedom Act as a means to help Internet users in repressive states. In 2008, the Global Online Freedom Act was passed by three House committees.

In the last dozen years, the Internet, in many countries, has been transformed from a freedom plaza to big brother's best friend. The technologies to track, monitor, block, filter, trace, remove, attack, hack, and remotely take over Internet activity, content, and users has exploded. Many of these technologies are made in the United States. Many of them have important and legitimate law enforcement applications, but sadly, many of them are also being exported every day to some of the most unsavory governments in

the world whose use of them is far from legitimate. Every day we learn that more activists are being arrested for the use of newly developed technologies—much of it American technology—in China, Belarus, Egypt, Syria, and many other countries around the world. The stakes are life and death for online democracy activists, and they deserve our support and protection.

For example, Belarus is blocking social networking sites like Twitter and Facebook and aggressively shutting down opposition Internet sites. Kazakhstan, which already blocks a number of popular blogs and media sites, is also in the process of creating a "national Internet" where all domestic domain names will have to operate on physical servers within its borders. Syria is using sophisticated tools to limit the ability of the opposition to organize, and to track down peaceful protestors.

China has created the Great Firewall and wants to create its own sanitized version of the Internet that will essentially isolate China from much of what is happening in the rest of the world, and when protests break out, it simply shuts down the Internet, as it did in Tibet and Xinjiang in recent years.

In Vietnam, Facebook has been blocked for 2 years, and under a new executive decree, a number of bloggers and journalists who write for independent online publications have been arrested. Egypt continues to detain blogger Alaa Abd El-Fattah for his online criticism of the Egyptian army, and today we have just learned that in addition to its already extensive online censorship in Iran, the U.S. virtual embassy in Iran has been blocked after only 1 day of operation.

Today, I introduced a bill, along with Congressman Frank Wolf and some other Members of the House, a bill that responds to the growing use of the Internet as a tool of repression and to changes in technologies of repression. The new Global Online Freedom Act of 2011, H.R. 3605, fundamentally updates legislation I first introduced in 2006 and which in 2008, as I mentioned before, advanced through three House committees.

The new GOFA requires the State Department to beef up its reporting on Internet freedom in the annual Country Reports on Human Rights Practices and to identify, by name, Internet-restricting countries. This country designation will be useful not only in the diplomatic context, in helping to advance Internet freedom through naming and shaming countries, but will also provide U.S. technology companies with the information they need in deciding how to engage in repressive foreign countries.

Second, the bill requires Internet companies listed on U.S. stock exchanges to disclose to the Securities and Exchange Commission how they conduct their human rights due diligence, including with regard to the collection and sharing of personally identifiable information with repressive countries and the steps they take to notify users when they remove content or block access to content. This provision of the bill will help democratic activists and human rights defenders hold Internet companies accountable by creating a new, heretofore unrealized, transparency standard for Internet companies. This provision will also require foreign Internet service companies that are listed here in the U.S. to report this informa-

tion as well. This will include big Chinese companies such as Baidu, Sohu, and Sina.

Finally, in response to many reports that we have all seen in the papers recently of U.S. technology being used to track down or conduct surveillance of activists through the Internet or mobile devices, this bill will prohibit the export of hardware or software that can be used for potentially illicit activities such as surveillance, tracking, and blocking to the governments of Internet-restricting countries. Current export control laws do not take into account the human rights impact of these exports, and therefore do not create any incentive whatsoever for U.S. companies to evaluate their role in assisting repressive regimes.

This section will not only help stop the sale of these items to repressive governments, but will create an important foreign policy stance to the United States that will help ensure that dissidents abroad know that we are indeed on their side and that U.S. businesses are not profiting from this repression.

This export control law is long overdue and thoroughly consistent with the approach Congress has taken, for example, in restricting exports of certain crime control equipment to China. It makes no sense for us to allow U.S. companies to sell technologies of repression to dictators and then turn around and have to spend millions of dollars to develop and deploy circumvention tools and other technologies to help protect dissidents from the very technologies that U.S. companies exported to their persecutors.

Today's hearing is an important moment to take stock of where we are and how we can move forward to promote and defend Internet freedom around the world. What we do here in the United States is critically important to achieving our goals. We must send a strong message to companies; that they have a unique role to play in preserving online freedom and send an even stronger message to repressive governments that the Internet must not become what it is today, so often a tool of repression.

I would like to yield to my good friend and colleague, Mr. Payne, for any opening comments.

Mr. PAYNE. Thank you very much, Chairman Smith, for calling this very important and timely hearing that looks at the promotion of Internet freedom around the world. I would also like to thank our distinguished witnesses for agreeing to testify here this afternoon.

For over 2 billion people worldwide, the Internet serves as a daily source of news, a way to communicate with family and friends, and a place to conduct business. It has become a staple of our day-to-day lives around the world. For some, the Internet serves as a venue to express one's religious or political views, a right that we as Americans hold in the highest regard. It is in this capacity that the Internet has served as a tool for both freedom and repression.

Over the past year, we have witnessed what has been dubbed the Arab Spring. In countries throughout the Arab world, via the Internet and social networking, citizens have communicated, organized, and raised awareness of their plight under repressive regimes, oppressive regimes. Sites such as Facebook and Twitter have played a major role in these uprisings, offering the opportunity to spread

ideas and organize events with a large number of participants. In a March poll of Egyptian and Tunisian Facebook users, 85 percent of the respondents in both countries said that the primary use of Facebook was to raise awareness amongst countrymen, inform the global community or organize movements. Given that in the first quarter of 2011 the number of Facebook users in the Arab world increased by 30 percent, it is obvious the dramatic impact Facebook is having on these movements.

It should be noted that Facebook and other social media network sites still have a low penetration rate in these regions. In Egypt, for example, Facebook is used by a mere 5.5 percent of the population. However, this still amounts to 6 million users. It may be the case that Facebook users organized online and then grew protests through other means. I am interested in hearing from our panelists their thoughts on this issue.

Whether you view the Internet as a social networking site, as an instigating factor or simply a tool, one thing is clear, the long-suspected power of the Internet to bring about political change has been confirmed, and that is very good. The world watched as Egyptians took to the streets to demand a new government. In what has been called the Facebook revolution, on February 11th, citizens from all around the globe celebrated as President Hosni Mubarak stepped down after 29 years of power. In Yemen, one activist who worked to organize protests through social media explained that the Internet served to break the fear and the silence and that online he felt freer to express his opinion. Just a few weeks ago Yemen's dictator of 33 years, Ali Abullah Saleh resigned.

In other countries, the outcomes were bleaker or the protest continues. The prevalence of uprisings have caused governments to enact stricter policies against political dissent and further restrict access to information in online networking tools. Former President Clinton once said trying to control the Internet would be like trying to nail Jell-O to the wall. Unfortunately, there are repressive regimes around the world that are attempting to do just that, and some with relative success.

I recently visited Bahrain where reports surfaced that the government deliberately blocked bloggers' sites and is restricting its citizens from accessing Internet, access to sites like Facebook, Yahoo!, YouTube, and Google Earth, yet determined to share their stories, protestors and bloggers still accessed the Internet.

In Syria, where there is limited freedom of the press, the Syrian Government monitors Internet use very, very closely and has detained civilians for expressing their opinions or reporting information online. Yet activists are using an iPhone application to disseminate news and information online about their protests against Assad.

While the Internet and mobile technology have allowed the voices of dissent to be heard even when governments attempt to block them, there is no doubt that for authoritarian regimes, the Internet has become the new platform for oppression.

In China, the government is aggressively censoring online content to its 450 million users. According to the State Department's 2010 Human Rights Report, an estimated 70 Chinese civilians are currently in prison for the political statements they wrote online.

This is totally wrong. Through these activities, China has managed to instill fear in users and providers, leading to self-censorship, yet many brave bloggers are continuing to share their stories online.

In Zimbabwe, Mugabe's aligned police forces arrested and charged 46 people with treason for watching a video of Egypt and Tunisia's protests this past February. I am confident that everyone in this room condemns the action of China, ZANU–PF and others in their attempt to restrict the spread of information within their borders. We all support the notion of freedom of speech and freedom of information. We strongly believe that it is wrong to prosecute and incarcerate individuals for expressing their political views. China and ZANU–PF undoubtedly defy many of our Nation's principles and deny basic human rights to its people in a number of areas.

However, as the United States seeks to promote these democratic values throughout the world, we must be sure that our initiatives do not hurt those who they are intended to protect. So in dealing with these issues, it is important that we maintain a level head and respond rationally. Our conversation should be about asking the question: How can we best serve the citizens of these countries? Once our course is decided, and initiatives implented, we must continue to monitor and evaluate the impact of our policies to ensure that they have the intended impact.

In February, just days after President Mubarak resigned, Secretary Clinton confirmed the U.S. commitment to a free and open Internet. By the end of this year, through the Net Freedom Task Force, the U.S. will have contributed $70 million in projects to promote Internet freedom globally since 2008. This does not include initiatives of the Broadcasting Board of Governors, who have contributed $2 million a year over the past decade, toward granting access to its Web site via proxy servers.

I hope to learn how the U.S. can improve on its endeavor to create an open and free Internet, and I am also interested in hearing how information is being restricted in African countries like Ethiopia and Zimbabwe. There have been reports that China was providing hardware and technical assistance to these governments in Zimbabwe and Ethiopia with the goal of jamming political opposition radios and monitoring emails. I look forward to hearing from our witnesses, and I thank you again for your willingness to testify.

Mr. SMITH. Thank you, Mr. Payne. I would ask unanimous consent that all witnesses' testimonies be accepted, and complete written testimonies be included in the record, and any extraneous material they would like to affix to their testimonies. Without objection, so ordered. I would also, without objection, would ask that the full biographies of each of our distinguished witnesses be included in the record, the very rich and varied backgrounds, great academic accomplishments, but because I want to get right to the testimony, I will give a very short introduction.

Beginning first with Dr. Daniel Calingaert who oversees Freedom House's contributions to policy debate on democracy and human rights issues and public outreach. He previously supervised Freedom House's civil society and media programs worldwide. Dr. Calingaert contributes frequently to policy and media discussions on democracy issues, including Internet freedom and authoritarian

regimes. Prior to joining Freedom House, Dr. Calingaert was associate director of American University's Center for Democracy and Election Management and associate director of the Commission of Federal Election Reform.

We will then hear from Ms. Clothilde Le Coz, who is the Washington director for Reporters Without Borders, where she works to promote press freedom and free speech around the world. Previously she was in charge of Reporters Without Borders Internet Freedom Desk and focused on China, Iran, Egypt, and Thailand. She also updated the organization's handbook for bloggers and cyber dissidents published in 2005. Her role is now to raise awareness of the constant threats that journalists are subjected to in many countries.

Then we welcome back to the committee a woman who has been here many times, Ms. Elisa Massimino, who has been the president since 2008 and chief executive officer of Human Rights First, one of the Nation's leading human rights advocacy organizations. Ms. Massimino helped establish the organization's Washington office in 1991 and served as the Washington director from 1997 to 2008. She is a national authority on human rights law and policy, has testified, as I indicated, dozens of times, and has published frequently. In 2008, the Washington newspaper, The Hill, named Ms. Massimino one of the top 20 public advocates in the entire country.

Then we will hear from Ms. Rebecca MacKinnon, who is again welcomed back to the committee to speak so authoritatively on this subject, is a senior fellow at the New America Foundation where she focuses on U.S. policies related to Internet, human rights, and global Internet freedom. She is cofounder of Global Voices Online, a global citizen media network and a founding member of the Global Network Initiative, a multi-stakeholder initiative to advance principles of freedom of expression and privacy in the information and communications technology sector. She is a former journalist for CNN in Beijing and Tokyo. Her first book, "Consent of the Networked," will be published next month.

So, Dr. Calingaert, if you could begin your testimony. Just let me—Congresswoman Ann Marie Buerkle, a member of the subcommittee, has arrived. Do you have a statement?

Ms. BUERKLE. Thank you, no, I will yield my time, but I thank you for holding this very important hearing.

Mr. SMITH. Thank you, Ms. Buerkle.

STATEMENT OF DANIEL CALINGAERT, PH.D., VICE PRESIDENT, FREEDOM HOUSE

Mr. CALINGAERT. Mr. Chairman, honorable members, thank you very much for the opportunity to testify today. Authoritarian regimes have imposed extensive restrictions on Internet freedom. These restrictions are well documented in Freedom House's report, "Freedom on the Net," and by others. I would ask that this Freedom in the Net report be entered into the record.

Mr. SMITH. Without objection, so ordered.

Mr. CALINGAERT. I would like to focus on the use of Western technology to restrict the Internet and on the U.S. Government's response. Almost every regime affected by the Arab Spring has used U.S. or European technology to suppress pro-democracy move-

ments. Over the past several months investigative reports by Bloomberg News, The Wall Street Journal, and analysis by the OpenNet Initiative have documented a number of cases. Boeing subsidiary Narus sold monitoring technology to Telecom Egypt, NetApp software was part of a surveillance system installed in Syria, technology from Blue Coat Systems ended up in Syria. Blue Coat sold technologies to Bahrain, Qatar, and the United Arab Emirates. There were also important European cases, British company Gamma provided technology to Egypt's Interior Ministry under former President Mubarak to record Skype conversations. A French firm, Bull, installed a sophisticated Internet monitoring center in Libya while Colonel Ghadafi was in power, an Italian company, Area, installed an Internet surveillance system in Syria.

The list goes on, and you can get the full list in my written testimony. But these are just the reported cases of U.S. and European technology that has ended up in the hands of Arab governments that restrict the Internet. There probably are many more. When these companies were asked by news reporters who their clients are, they usually refused to answer.

Advanced technology for monitoring online data and communications attracts a great deal of interest overseas. A conference that brought together buyers and sellers of this technology this year in Dubai nicknamed the Wiretappers Ball had about 1,300 people in attendance. The Middle Eastern governments that have acquired Western technology for Internet censorship or surveillance have abysmal human rights records. Of the countries I have listed before, all but one were rated not free by Freedom House for calendar year 2010. Two of them were among the worst of the worst.

Western technologies are working directly at cross-purposes with U.S. Government policy to promote Internet freedom. The U.S. Government is supporting efforts to circumvent Internet censorship at the same time as Western technology is making that censorship more robust, and the U.S. Government is funding programs to train human rights and pro-democracy activists in digital security while U.S. and European companies are selling surveillance software that puts those very same activists at greater risk.

I give credit to the administration for the good work it has done on Internet freedom, but in dealing with the specific challenge of U.S. technology exports, the administration, frankly, has dropped the ball. The administration's approach to this challenge can be summed up in one line from Secretary Clinton's speech in February on Internet rights and wrongs. She said that businesses have to choose whether and how to enter markets where Internet freedom is limited. In essence, she is telling U.S. businesses to just do the right thing, but U.S. businesses continue to sell surveillance and censorship technologies to some of the worst abusers of human rights.

Stronger action is needed. The Global Online Freedom Act is very much needed to stop the complicity of U.S. companies in suppressing Internet freedom. A key provision of GOFA is to prohibit exports of surveillance and censorship technology to countries that restrict the Internet. During recent protests in Cairo, angry Egyptian demonstrators held up U.S.-made tear gas canisters as a sign that the United States was still supporting their oppressors.

Similarly, the use of U.S. technology by repressive regimes to track down democracy advocates who are then imprisoned and tortured is a blemish on America's image and a blow to U.S. credibility. GOFA would also promote transparency by requiring U.S. technology companies to disclose how they block online content and collect and share personal data. This requirement would make the companies more accountable to their users and encourage U.S. companies to push back on requests to collaborate with Internet censorship and surveillance. The trade provisions of GOFA merit strong support as well. They would push the U.S. Trade Representative to challenge Internet censorship more forcefully and stand up for U.S. companies that are adversely affected. Trade negotiations offer an effective way to promote the free flow of information.

The U.S. Government and European governments have launched significant initiatives to protect online freedom, but these initiatives by themselves cannot keep pace with the growing Internet restrictions imposed by repressive regimes. Stronger actions are needed to stem the decline in global Internet freedom and to enable hundreds of millions of Internet users around the world to exercise their fundamental rights online. Thank you.

Mr. SMITH. Dr. Calingaert, thank you very much for your testimony and for your recommendations and for the insights and counsel you have provided to us as we shape this legislation.

[The prepared statement of Mr. Calingaert follows:]

Testimony of Daniel Calingaert
Freedom House Vice President for Policy

Subcommittee on Africa, Global Health, and Human Rights
Committee on Foreign Affairs
U.S. House of Representatives

"Promoting Global Internet Freedom"

December 8, 2011

Mr. Chairman, Honorable Members, thank you for the opportunity to testify before your subcommittee today. This hearing is taking place against the backdrop of a steady decline in global internet freedom. Repressive regimes are exerting ever stronger control over the internet, and they are being assisted by U.S. and European companies. They are using technologies made in the United States and in Europe to censor internet content, such as independent news websites, and to monitor the online activities of dissidents and human rights defenders.

The U.S. and European governments have pursued significant initiatives to protect online freedom, but these initiatives are inadequate to stem, let alone reverse, the decline in freedom on the internet. Stronger action is needed.

Restrictions on Internet Freedom

Well before the Arab Spring, the power of the internet to expand space for free expression was well known. That power was all the more evident during the popular uprisings across the Middle East and North Africa. The internet accelerates the free flow of news and views and brings like-minded citizens together to mobilize for change.

Authoritarian regimes are well aware of the internet's power and began years ago to introduce extensive controls over digital media. Some of them, including China, Iran, Saudi Arabia, and Vietnam, have built pervasive, multilayered systems for online censorship and surveillance. These systems consist of blocks on access to social media applications, technical filtering of internet content, human censorship, outsourcing of censorship and surveillance to private companies, clandestine use of paid pro-government commentators, intercepts of emails and other online communications, arrests and prosecutions of cyber-dissidents, intimidation of bloggers

and online journalists, and digital attacks on opposition and independent news websites. In the past two years, as documented in Freedom House's *Freedom on the Net* 2011 report and elsewhere, these systems for control of the internet have grown more diverse and more sophisticated.

Governments increasingly resort to "just-in-time" blocking of online content or social media applications at critical moments, such as periods of unrest. Malawi's government, for example, blocked access to news websites, Facebook, and Twitter in July as part of its clampdown on mass protests. Just-in-time blocking at times has affected a whole country's internet. Access to the internet was cut off entirely in Egypt amidst the January 2011 mass protests calling on then President Hosni Mubarak to step down and in Libya in March 2011 as its leader, Muammar Qaddafi, tried to stem the anti-regime uprising.

Moreover, government control of internet infrastructure is increasingly being used to insulate citizens from the global internet. Iran, for instance, is taking steps toward the creation of a national internet to disconnect Iranian users from the rest of the world.

Intermediary liability is on the rise as a method of censorship. Governments increasingly hold hosting companies and service providers liable for the online activities of internet users. Intermediary liability is a central component of China's robust censorship apparatus and is spreading in other countries. In Vietnam and Venezuela some webmasters and bloggers have disabled the comment feature on their sites to avoid potential liability. Governments also force businesses to police internet use. Belarus, for example, introduced requirements for Internet cafés to check the identity of users and keep a record of their web searches.

Online surveillance appears to have grown more extensive over the past two years. In Iran, for example, the government used intercepted online communications, including activities on Facebook and the Persian-language social media site Balatarin, to prosecute activists involved in protests against the fraudulent 2009 presidential election. Many arrested activists reported that interrogators confronted them with copies of their emails, demanded the passwords to their Facebook accounts, and questioned them about individuals on their friends list. Online surveillance has spread beyond dissidents. In China, Thailand, and elsewhere, ordinary citizens who never considered themselves activists were detained or investigated because of tweets they made, emails they sent to friends, or content they downloaded at an internet café. These citizens just happened to circulate or download information that the government found objectionable.

Digital attacks against human rights and democracy activists have become widespread. The pro-regime Syrian Electronic Army defaced Syrian opposition websites and spammed popular Facebook pages, including that of U.S. President Barack Obama, with pro-regime messages. Sophisticated cyber attacks have also originated from China. These included denial-of-service attacks on domestic and overseas human rights groups, email messages to foreign journalists containing malicious software capable of monitoring the recipient's computer, and a cyber-espionage network, which extended to 103 countries, to spy on the Tibetan government-in-exile.

In Belarus, to stifle protests against the fraudulent December 2010 elections, denial-of-service attacks slowed down connections to opposition websites or rendered them inaccessible. The

country's largest internet service provider, the state-owned Belpak, redirected users from independent media sites to nearly identical clones that provided misleading information, such as the incorrect location of a planned opposition rally. Digital attacks on websites or blogs that are critical of the government have also taken place in several countries rated "partly free" on internet freedom by Freedom House, including Kazakhstan, Malaysia, and Russia.

U.S. and European Technologies

Repressive regimes in the Middle East and elsewhere are acquiring U.S. and European technologies to extend their control over the internet. Almost every regime affected by the Arab Spring has used U.S. or European technology to suppress pro-democracy movements. Over the past several months, investigative reports by Bloomberg News and the Wall Street Journal and analysis by the Open Net Initiative have documented the following cases:

- Boeing subsidiary Narus sold technology for monitoring emails and other online communications to the state-run Telecom Egypt.

- Email archiving software produced by Silicon Valley-based company NetApp Inc. was part of a surveillance system installed in Syria under the direction of intelligence agents. The company denies knowledge of the re-sale of its products to Syria.

- Technology of another Silicon Valley-based company, Blue Coat Systems Inc., to censor the internet and record browsing histories, ended up in Syria, apparently without the company's knowledge.

- Blue Coat sold technology to Bahrain, Qatar, and the United Arab Emirates (UAE) to block websites.

- Websense Inc. of San Diego, California sold technology to Yemen's government-run internet service provider, which filtered political and social online content.

- SmartFilter products of McAfee, which is owned by Intel, are used in Saudi Arabia, UAE, Kuwait, Bahrain, and Oman to block access to websites that provide critical views of Islam or tools for anonymous online activity. The Tunisian government of former President Ben Ali used SmartFilter products as well.

- British company Gamma provided technology to Egypt's Interior Ministry under former President Mubarak to hack personal accounts on Skype and record voice conversations.

- French technology firm Bull SA installed a sophisticated internet monitoring center in Libya while Col. Gadhafi was in power. This center intercepted emails of human rights and opposition activists.

- Italian company Area SpA installed an internet surveillance system in Syria.

- Spyware was sold to Bahrain by German electronics giant Siemens and maintained by another German company, Trovicor GmbH.

- Milan-based company HackingTeam has sold technology for bypassing Skype's encryption and intercepting audio streams to about two dozen policy or security agencies in unnamed countries of the Middle East, North Africa, and Far East.

- Canadian firm Netsweeper Inc. has provided the national internet service providers of Qatar, UAE, and Yemen with filtering technology, which was used to censor political and religious content.

These are just the reported cases of U.S. and European technology for internet censorship and surveillance that has ended up in the hands of Arab governments that restrict the internet. There probably are many more cases. In the news articles about this technology transfer, U.S. companies are asked who their clients are, and they usually refuse to answer.

Sales of advanced technology for monitoring online data and communications are estimated to amount to $5 billion a year, according to a December 1 story in the Washington Post. This technology is sold at conference around the world, nicknamed the Wiretappers' Ball, which attract hundreds of vendors and thousands of potential buyers. The most popular conference this year was in Dubai; it had about 1,300 people in attendance.

Online surveillance technology is commonly used by law enforcement in the United States and other democratic countries and is critical for thwarting terrorists and criminals. It is generally a benefit to society where due process applies. Independent media can expose any misuse of the technology, and courts can ensure that online surveillance in conducted in accordance with the law. However, in countries where there is little respect for the rule of law, online surveillance technology is used to violate the rights of internet users and to facilitate human rights abuses, and censorship technology strengthens restrictions on free expression.

The abysmal human rights records of the governments that have received Western censorship and surveillance technology is cause for serious concern (all of the countries cited above were rated "not free" by Freedom House for calendar year 2010, except for Kuwait, which was "partly free"). These governments routinely restrict peaceful political speech. They harass and arrest dissidents and allow the torture of prisoners. Censorship and surveillance technology facilitated these human rights abuses. The report of the Bahrain Independent Commission of Inquiry, for example, documented cases where intercepted emails where used in interrogations of citizens who were mistreated or tortured.

Western technologies to restrict the internet are working directly at cross-purposes with U.S. government policy to promote internet freedom. The U.S. government supports civil society's efforts to challenge internet restrictions in repressive environments, including to circumvent internet censorship and to strengthen digital security of human rights and pro-democracy activists. U.S. and European companies meanwhile are bolstering the censorship that U.S.-supported activists are trying to circumvent and making these activists more vulnerable to the online surveillance they are trying to evade.

Current Support for Online Freedom

The Obama Administration has made internet freedom a priority in U.S. foreign policy and a key component of its human rights agenda. It has presented a clear set of policy goals for promoting freedom of expression online, undertaken diplomatic efforts to pursue these goals, and allocated substantial resources to counteract restrictions on the internet. European governments, led by Sweden and the Netherlands, have developed similar policies to advance internet freedom. U.S. and European policies generally pursue the following aims:

- ***Preserve open nature of internet*:** The U.S. and European governments have resisted attempts to place Internet governance under the United Nations, specifically the International Telecommunication Union, where authoritarian regimes may have greater scope to control online space. They instead support the multi-stakeholder bodies that currently govern the Internet, such as the Internet Corporation for Assigned Names and Numbers (ICANN).

- ***Expand international recognition for key principles of free expression online*:** Forty-one governments have agreed on the principle, as expressed by Swedish Foreign Minister Carl Bildt, that "The same rights that people have offline—freedom of expression, including the freedom to seek information, freedom of assembly and association, amongst others—must also be protected online." This principle was reaffirmed and elaborated by United Nations Special Rapporteur for Freedom of Expression, Frank La Rue, in his report on Internet freedom to the UN Human Rights Council in June 2011.

- ***Support digital activists*:** The Netherlands and Sweden have begun to fund programs to support bloggers and cyber dissidents who come under threat. They have also pushed for greater European Union funding for internet freedom programs. The U.S. State Department has supported a range of initiatives to promote digital activism and spoken out against the arrests of prominent bloggers, such as Bahraini "blogfather" Mahmood al-Yousif.

- ***Fund anti-censorship technologies and digital security*:** The U.S. State Department has spent $70 million since 2008 on a range of Internet freedom programs. These programs have included support for technologies to circumvent online censorship, secure mobile phone tools, efforts to reintroduce blocked content to users behind a firewall, and training for activists in digital security. (Freedom House's internet freedom programs are funded in part by the U.S. State Department, Swedish International Development Agency, and Dutch Foreign Ministry.)

However, U.S. and European policies on internet freedom have significant limitations. Little is being done to stop the use of U.S. and European technologies to facilitate internet censorship and surveillance. Secretary of State Hillary Clinton, in February 2011 speech on "Internet Rights and Wrongs," exhorted technology companies to act responsibly. She said that "Businesses have to choose whether and how to enter markets where Internet freedom is limited." She looked to the Global Network Initiative (GNI), which brings together businesses and human rights groups, to

"solve the challenges" that repressive regimes pose to U.S. technology companies. GNI has promoted better human rights practices among some companies but has failed to stem the sales of Western surveillance and censorship technologies to some of the worst abusers of human rights.

The initiative of Senators Mark Kirk, Robert Casey, and Christopher Coons to press for investigation of the sales of NetApp and Blue Coat technologies to Syria is welcome. Such an investigation will serve to determine whether NetApp and Blue Coat violated U.S. sanctions on Syria and encourage U.S. companies to take steps to prevent their technologies from ending up in sanctioned countries. However, this initiative is insufficient to stem the sales of U.S. censorship and surveillance technologies, because it is focused on Syria alone and applies only to the handful of countries that are under U.S. sanctions.

Strengthening Internet Freedom

The growing internet restrictions imposed by repressive regimes are outpacing U.S. and European efforts to protect the space for free expression online. To expand this space, the U.S. government and our European allies need to build on current policies with additional initiatives.

Export Controls

The best place to start in bolstering U.S. policy is with the updated Global Online Freedom Act, introduced this week in the U.S. House of Representatives as "GOFA 2.0." This bill is timely and necessary to curtail the collaboration of U.S. companies in the suppression of internet freedom.

A critical provision of this bill is the prohibition on exports of surveillance and censorship technologies to countries that restrict the internet. GOFA will move the United States beyond the current contradictory policies of offering support to pro-democracy activists while at the same time turning a blind eye to the sale of U.S. technologies that put those very activists at greater risk.

In Cairo during recent protests, angry Egyptian demonstrators held up U.S.-made tear-gas canisters as a sign that the United States was still supporting their oppressors. In much the same way, the use of U.S. technology by repressive regimes to track down democracy advocates, who are then imprisoned and tortured for espousing our common values, is a blemish on America's image and a blow to U.S. credibility.

Export controls may put a few U.S. businesses at a competitive disadvantage, but they are the only effective way to stop the use of U.S. technology to violate human rights. They can be carefully targeted to have a limited impact on U.S. commercial interests. Export controls should apply only to specific technologies, such as spyware and content filters, that serve the primary purpose of monitoring digital communications or blocking online content or to technologies that are specifically configures for these purposes.

GOFA 2.0 dovetails with efforts in Europe to curb similar technology sales. Dutch Foreign Minister Uri Rosenthal has called for export controls on technologies that filter Internet content, and the European Parliament voted in April to introduce controls on technologies for monitoring Internet and mobile-phone use, though these measures still require the European Council's approval.

Transparency

U.S. technology companies often come under pressure from authoritarian regimes to facilitate violations of human rights, for instance to filter online content or to provide access to private user data or communications. Google, in its Transparency Report, discloses the number of requests it receives from different governments to remove content or to hand over user data. Other technology companies have yet to follow Google's good example.

Thus, little is known about what U.S. technology companies do to maintain a free flow of information when faced with pressure from authoritarian government censors or to protect user data against foreign state security agents who are going after peaceful dissidents. These companies are unlikely to stand up to the pressure unless they have to answer for their actions.

The Global Online Freedom Act would require U.S. technology companies to disclose how they block online content and collect and share personal data. This requirement would make the companies more accountable to their users for how they handle user privacy and thereby would encourage U.S. companies to push back on requests to collaborate in internet censorship and surveillance.

Trade Negotiations

In October, the U.S. Trade Representative (USTR) announced its request for information under World Trade Organization rules for information about China's internet restrictions. The request aims to ascertain whether blocking of websites outside of China constitutes a trade barrier.

USTR previously had shied away from trade disputes over internet censorship. The October announcement is a welcome first step, but more is needed. GOFA would encourage USTR to become more proactive in using trade rules and negotiations to promote the free flow of information online. It would require USTR to report to Congress on trade disputes related to internet censorship by foreign governments and on USTR efforts to address those disputes. Trade rules and regulations offer an effective way to promote the free flow of information online, because the potential loss of trade that China and other countries might suffer as a result of a trade dispute gives them a strong incentive to curb their internet censorship.

Beyond GOFA

In addition to current policy and to GOFA, the United States should more proactively challenge restrictive internet laws and practices abroad. These laws and practices often go unchallenged. U.S. officials were largely silent, for instance, when Saudi Arabia introduced a requirement in early 2011 for online media sites, including blogs, to obtain a license to operate.

The State Department, in collaboration with our European allies, should also develop an action plan to implement the recommendations of UN Special Rapporteur Frank La Rue's report on internet freedom. This plan should aim to curb restrictions on internet content, criminal penalties for legitimate online expression, intermediary liability, infringements on online privacy, and cyber attacks.

Every aspect of U.S. policy on internet freedom is more effective when conducted in concert with our democratic allies. Joint diplomatic initiatives would make greater progress in promoting respect for international principles of free expression, defending bloggers and cyber activists who come under threat, and challenging restrictive internet laws and practices. Coordination on trade disputes would place greater pressure on authoritarian governments to refrain from internet censorship, and export controls would have greater impact if they were applied equally to companies in all democratic countries.

As we speak, the Dutch Foreign Ministry is convening a major conference in The Hague on Freedom Online. This conference brings together multiple stakeholders—government ministers and senior officials, leaders of technology companies, and civil society representatives—to discuss many of the same issues we are raising here today. It is a valuable opportunity to strengthen trans-Atlantic collaboration on internet freedom.

To advance internet freedom in the face of growing restrictions around the world, the U.S. government needs to do more. It cannot rely entirely on advocating broad principles, criticizing flagrant abuses, and funding programs. It has to take bolder actions, particularly to require greater transparency by U.S. companies and to introduce export controls on U.S. technology to repressive regimes to censor online content and monitor private digital communications. Such actions are critical to reverse the global decline in internet freedom and to enable hundreds of millions of internet users around the world to gain greater freedom to express their views openly online.

Thank you for your attention.

Mr. SMITH. Next, Ms. Le Coz, if you could present your testimony.

STATEMENT OF MS. CLOTHILDE LE COZ, WASHINGTON DIRECTOR, REPORTERS WITHOUT BORDERS

Ms. LE COZ. Thank you, Mr. Chairman. I would like to thank the subcommittee for organizing this very timely hearing as well as you, Mr. Chairman, for your commitment to promote global Internet freedom. For the past 4 years, I have been working on that topic, and this is a great opportunity to reiterate how online freedom is bound to the fundamental right to freedom of expression, but also to insist on the fact that human rights cannot be isolated from the other political and economic issues at play, and we welcome the new GOFA in that sense.

The years 2010 and 2011 firmly established the role of social networks and the Internet as mobilization and news transmission tools. The Arab Spring and the echoes it had in Asia and Latin America made it clear that the Internet on computers and mobile phones was a very powerful tool of expression and witness. But unfortunately, it also made it very clear that what could be said and published could also be censored and attacked.

Since the beginning of 2011, online censorship and restrictions are actually more important than before in some of the countries. For example, China did add the keyword "Jasmine" to their blacklist, as they even did with the word "occupy." Vietnam reinforced the sanctions against bloggers and reporters' activities, and the authorities even threatened two netizens with possible imprisonment after they urged Vietnamese to follow the example of pro-democracy demonstrators in the Middle East.

But China and Vietnam are definitely not the only ones following this trend, and what we witnessed today in Egypt, for example, can be compared to the Mubarak era methods. Alaa Abd El-Fattah and Maikel Nabil Sanad, certainly two of the most prominent bloggers, have been arrested simply for expressing their views, and they are still in jail, and in Syria, the Internet slows down every Friday when the main weekly demonstration takes place.

Promoting global Internet freedom is first and foremost being able to link this issue to trade because there is a criminal cooperation between Western high tech companies and authoritarian regimes. According to Reporters Without Borders, more than 120 netizens are behind bars simply because of what they wrote online, and at least a dozen European and American companies have helped their government to put them in jail.

According to files released by WikiLeaks in partnership with five news media outlets last week, more than 160 companies are actually involved. The surveillance tools sold by these companies are used all over the world by armed forces, intelligence agencies, and democratic and repressive governments. Any computer or mobile phone can be physically located.

The United States took the lead, the main lead, in promoting online Internet freedom together by making clear that companies have a responsibility and should have a responsibility when selling their technologies abroad, and the United States should continue to do so, but American actions abroad cannot be relevant if the

United States are not applying domestically what they are promoting internationally, and in the past year, however, one major issue has been of concern for online freedom in the U.S. Recently two bills were introduced that, if passed, would prevent the American citizens to benefit from this freedom. Aimed at fighting criminal behavior, which we obviously agree on, the Stop Online Piracy Act and the Protect IP Act would have serious implications for international civil and human rights.

Some provisions are actually instituting DNS filtering and making it possible for Web services to take deliberate actions to prevent the possibility of infringement from taking place on their sites. That means that wrongly accused Web sites could therefore directly suffer from this action. And DNS filtering very much contributes to the Great Firewall that prevents Chinese citizens to access free information. Therefore, in order to promote global Internet freedom, our organization is asking today the U.S. Congress to reject the Stop Online Piracy Act and the Protect IP Act, but mostly to adopt effective measures to prevent the export of technology, equipment, and software to countries where they are likely to be used to violate freedom of expression and human rights, and this is what we think the new GOFA will help, and also to encourage companies, U.S. companies to ensure that the equipment supplied to a permitted country is not subsequently transferred to one that it is not.

Reporters Without Borders would also like the U.S. Congress to encourage other countries, not only the U.S., but other countries to do so because this is one of the ways it could really be effective.

And, lastly, is also asking not to keep human rights and online freedom on the site when talking about trade. This is exactly what we think GOFA will help to do, and last October, China's restriction on the Internet have led to the U.S. ambassador to the World Trade Organization to complain about China's firewall on the grounds that it was violating WTO rules. Thank you.

Mr. SMITH. Ms. Le Coz, thank you so very, very much.

[The prepared statement of Ms. Le Coz follows:]

1500 K street NW
Suite 600
Washington, DC 20005
202 879 9295

Promoting Global Internet Freedom
Written Statement by

Clothilde Le Coz
Washington DC Director

I would like to thank the Subcommitte for organizing this very timely hearing as well as Congressman Smith for his commitment to promote global Internet freedom. I have been working on this topic for the past 4 years and today is a great opportunity to reiterate how online freedom is bound to the fundamental right to freedom of expression.

Just this week, at least 15 websites critical of the Russian government were paralyzed before and during the parliamentary elections by a series of Distributed Denial of Service (DDoS) attacks, aimed as silencing them. As most of the traditional media, including TV stations, are controlled by the Kremlin, real political debate takes place only online. But coordinated cyber-attacks and arrests of journalists and bloggers were carried out in an apparent bid to suppress even the online debate.

But by creating new spaces for exchanging ideas and information, the Internet is a force for freedom. In countries where the traditional media are controlled by the government, the only independent news and information are to be found on the Internet, which has become a forum for discussion and a refuge for those who want to express their views freely.

However, more and more governments have realized this and are reacting by trying to control the Internet. Never have so many countries been affected by some form of online censorship, whether arrests or harassment of netizens, online surveillance, website blocking or the adoption of repressive Internet laws. Netizens are being targeted by government reprisals. Around 127 of them are currently detained for expressing their views freely online, mainly in China, Iran and Vietnam.

The years 2010 and 2011 firmly established the role of social networks and the Internet as mobilisation and news transmission tools. In 2010 alone, 250 million Internet users joined Facebook and by the end of the year, the social network had 600 million members. In September that year, 175 million people were Twitter users – 100 million more than in the previous year.

The Western media had praised the Internet and its "liberator" role during the 2009 Iranian revolution. According to *The New York Times*, the demonstrators "shot tweets" back at bullets. However, Twitter was then used mainly by the diaspora. "The Net Delusion," a theory advanced by Evgeny Morozov, an Internet expert, casts doubt on the Internet's role as a democratisation tool. Although the Internet is certainly used by dissidents, it is also used by the authorities to relay regime propaganda and enforce a police state.

Repressive regimes have intensified censorship, propaganda and repression, keeping netizens and journalists in jail. But repressive regimes are not the only ones trying to get a tighter hand online. Issues such as national security - linked to the WikiLeaks publications - and intellectual property - are also challenging democratic countries' support to online free speech.

The Arab Spring - the web reached new heights at high costs

The terms "Twitter Revolution" and "Facebook Revolution" have become watchwords with the events that rocked the Arab world in late 2010 and early 2011. The "online" movements were coupled with "offline" demonstrations, hastening the fall of dictators. The Tunisian and Egyptian uprisings turned out to be, first and foremost, human revolutions facilitated by the Internet and social networks.

Facebook and Twitter served as sound boxes, amplifying the demonstrators' frustrations and demands. They also made it possible for the rest of the world to follow the events as they unfolded, despite censorship. The role of cell phones also proved crucial. Citizen journalists kept file-sharing websites supplied with photos and videos, and fed images to streaming websites.

The Tunisian authorities had imposed a media blackout on what was going on in Sidi Bouzid. Since the so-called "traditional" media had failed to cover the protest movements that were rocking the country, at least at their beginning in December, their role as news sources and vectors was taken over by social networks such as Facebook and Twitter, and news websites like Nawaat.org. Facebook in particular acted as a platform on which Internet users posted comments, photos and videos. The Bambuser streaming site also had its moment of glory. Everyone was able to track the events as they happened. The online calls for demonstrations spread to other countries: Egypt, Libya, Yemen, Bahrain, Oman, Syria, Iraq, Morocco, and even China and Vietnam, and elsewhere around the world.

China restricted even more online rules since the beginning of the growing movement. China now has half a billion Internet users. Facebook and Twitter are censored but Sina Weibo, the Chinese microblogging website, has more than 200 million users. The public's enthusiasm for the Internet and the government's fear of online protests has resulted in constant improvements in online censorship. Weibo, for example, now employs 100 people around the clock just to monitor the content being posted online, according to the magazine Forbes. Several new keyword combinations are being blocked online. "Jasmine," the adjective often applied to the revolution that toppled Tunisia's President Ben Ali, is also censored. The *China Digital Times* website has a list of some of the terms that are censored on the Chinese Internet. It is now also impossible to search for a combination of the word "occupy" and the name of a Chinese city, for example, "Occupy Beijing"(占领北京) or "Occupy Shanghai"(占领上海)...), because the authorities clearly fear the spread of the "Occupy Wall Street" movement.

This is an unfortunate trend that Reporters Without Borders also witnesses in Vietnam. In March 2011, two cyber-dissidents in their 60s were facing possible imprisonment for urging Vietnamese to follow the example of pro-democracy demonstrators in the Middle East. In January 2011, the government also ordered a new decree regulating journalists' and bloggers' activities. This decree, which was added to one of the world's most repressive legislative arsenals, notably provides for fines of up to 40 million dong (2,000 U.S. dollars), in a country where the average salary consists of about 126 U.S. dollars.

In March 2011, Reporters Without Borders published a list of the «Internet enemies» countries and the ones that are «under surveillance». Although Egypt seemed to be less repressive online in the first months of the revolt, the methods used today recall the Mubarak era. Numerous journalists and bloggers who tried to expose abuses by some members of the armed forces and the military police during the pro-democracy uprising were prosecuted before military tribunals. The most symbolic case is that of the blogger **Maikel Nabil Sanad**, sentenced in April to three years' imprisonment.. The conviction made him Egypt's first prisoner of conscience since the revolution. He was accused of insulting the armed forces, publishing false information and disturbing the peace for having published a report on his blog casting doubt on the army's perceived neutrality during the demonstrations in January and February. His appeal hearing was due to open on 4 October but kept being postponed.

We could state even harsher comments on Syria or Bahrain for example. The pro-democracy movement reached Bahrain in mid-February 2011. The netizen **Zakariya Rashid Hassan** died in detention on April 9 presumably after having been tortured. He was accused of moderating an online discussion forum. Twenty-one human rights activists and opposition members received long prison sentences from a military court on June 22, at the end of a mass trial meant to serve as an example and give a strong message. Among them was the blogger **Abduljalil Al-Singace,** head of the Al-Haq movement's human rights office. On his blog he had drawn attention to human rights abuses against Shi'ites and the lamentable state of public freedoms in his country. He was sentenced to life imprisonment. **Ali Abdulemam**, known as an Internet pioneer in his country, was sentenced in absentia to 15 years' imprisonment. Between June and September 2011 ?, the authorities blocked a certain number of websites such as PalTalk, an audio and video chat group whose Bahrain Nation chat room has been used by members of the opposition to communicate with each other, the site Bahrain Mirror which criticizes the government, the website of the Bahrain Justice and Development and Movement, founded in July this year, which highlights human rights violations in Bahrain and advocates democratic reform, and Twitcam which allows real-time streaming on Twitter.

In Syria, Internet service slows down on almost every Friday, when the main weekly demonstration takes place. This often lasts for a considerable amount of time to prevent videos shot during the rallies from being uploaded or transmitted. The cyber-army responsible for monitoring cyber-dissidents on social networking sites, appears to have stepped up its activities since the end of June. Its members flood sites and Web pages that support the demonstrations with pro-Assad messages. Twitter accounts have been set up to interfere with the hash tag #Syria by sending hundreds of tweets whose keywords are linked to sports results or photos of the country.

It also seeks to discredit the popular uprising by posting appeals for violence on the pages of government opponents, pretending that activists are behind them. As a means of monitoring dissidents, the authorities obtain personal details using phishing techniques, such as setting up false Facebook pages, or an invitation to follow a Twitter link to see a video. The unsuspecting user then enters an email address and password. Transmissions of the privately owned TV station Orient TV, which broadcasts from the United Arab Emirates, have been cut several times on the Nilesat and Arabsat satellites.

Therefore, Reporters Without Borders believes the outcome of the Arab Spring for online freedoms has to be balanced. Governments have shown their worse trends to control information. However, when Arab and some Asian leaders attempted to minimize reports of

violence and keep essential information from foreign journalists, local activists and researchers were on the ground to uncover the truth. Susan Rice, US Ambassador to the United Nations, acknowledged that, when gathering information on the Arab Spring, the Obama administration was relying on reports from " observers" since "journalists are banned".

There is truly no longer any reason for the long-lasting gap between the new and the traditional media. In the last few months, the new and traditional media have proven to be increasingly complementary. According to *BBC Global News* Director Peter Horrocks, it is imperative for journalists to learn how to use social networks: "It is not an option." The new media have become key tools for journalists. At the same time, by flooding social networks with news and pictures, Arab revolutionaries were also seeking to ensure that the international media covered news events in order to put pressure on their governments and on the international community. News staff now use Twitter and Facebook to find ideas for news stories, gather first-hand accounts and visuals, and to disseminate their own articles in order to expand their readership. The shelf life of an article no longer ends with the printing of a newspaper; it now has an extended life online.

WikiLeaks: Inevitable transparency and fear in democracies

This collaboration between the new and traditional media is exemplified by changes in WikiLeaks' strategy. Initially focused on the massive release of unedited confidential documents, the website gradually developed partnerships with several international media leaders ranging from *The New York Times* to *Le Monde*, and *The Guardian* to *Al-Jazeera*. This strategy allowed it to combine the new media's assets (instantaneousness and a virtually unlimited publishing capacity) with those of the traditional media (information checking and contextualisation, thanks to journalists specialised in the issues covered). More than 120 journalists of diverse nationalities worked together to decipher the diplomatic cables released by WikiLeaks, and to remove the names of civilians and local informants from said documents in order not to put them at risk. The series of close to 400,000 confidential documents belonging to the U.S. Army concerning the war in Iraq which WikiLeaks released helped to expose the magnitude of the crimes which coalition forces and their Iraqi allies had committed against civilian populations since 2003. Reporters Without Borders denounced the pressure that U.S. and Iraqi authorities have placed on the website and asked these two governments to demonstrate transparency and to reconsider their document classification methods.

Strong pressures are also being placed on WikiLeaks' collaborators. Founder **Julian Assange** has been repeatedly threatened. U.S. Army Private **Bradley Manning**, suspected of being one of WikiLeaks' sources, has been held in solitary confinement for several months and is facing life imprisonment. After being subjected to cyberattacks and being dropped by several host sites, WikiLeaks called upon its worldwide supporters on Dec. 5, 2010 to create mirror websites. Since December 2010 a number of media and websites – including *Le Monde*, *El Pais* and *Al-Quds Al-Arabi* in Morocco as well as *the Daily News* in Zimbabwe– were censored or sued for having relayed the cables. Access to the website is notably blocked in China and in Thailand. The site is accessible in Pakistan, but some pages containing wires about Pakistan are blocked. Even a hate campaign has been launched against journalists trying to relay some of the cables in Panama last May.

Setting aside the controversy that this publication created and just focusing on the content of these cables show that online media is seen as a growing threat by a growing number of

governments; repressive or democratic. For example, the arrest of the Malaysian blogger Raja Petra Kamarudin (RPK) in 2008 was both a way to pressure opposition leader Anwar Ibrahim and a warning to the growing online media. Then interior minister Syed Hamid himself publicly acknowledged that: "We have called and advised [RPK] many times following the publishing of his statements but he has continued to write." Deputy interior minister Wan Farid said that bloggers could not expect to be able to post "anything" without consequences and that RPK's arrest was a warning to all netizens.

In this context, where online repression can be equal to online expression, it is imperative that democracies stand up to promote online freedoms and make clear decisions and statements. In a historic speech on January 2010, U.S. Secretary of State Hillary Clinton referred to online freedom of expression as the cornerstone of American diplomacy – a position that she reasserted in February 2011 in an address where she reminded her audience: "On the spectrum of Internet freedom, we place ourselves on the side of openness." Nonetheless, the principles raised by Hillary Clinton conflict with the treatment reserved for WikiLeaks. Several days prior to WikiLeaks' publication of the documents, the Pentagon had asked the media "not to facilitate the leak" of classified documents concerning the war in Iraq, claiming that it would endanger national security. American officials made some very harsh statements about the site's founder. Judicial action may still be taken against the website. According to Hillary Clinton, "the WikiLeaks incident began with an act of theft" of government documents. However she stated that "WikiLeaks does not challenge our commitment to Internet freedom."

Promoting online freedom has to have relevant foundations and democracies seem to be the best political system so far to promote it. But apart from national security and cybersecurity, other problems are persuading democratic governments to relativise their commitment to a free Internet. France and Australia are already on the list of «countries under suveillance» for their attempts to control online contents for copyrights and pedophilia issues.

There is of course no excuse for people committing crimes and legal mechanisms have to be implemented to find if they are criminals. But with the implementation in France of the three-strikes legislation and of a law providing for the administrative filtering of the web and the defense of a civilised Internet, the impact of recent legislation and government-issued statements about the free flow of online information are raising serious concerns. In Australia, the government has not abandoned its dangerous plan to filter online traffic, even though this will be hard to get parliamentary approval. A harsh filtering system after a year of tests in cooperation with Australian Internet service providers, telecommunications minister Stephen Conroy said in December 2009 the government would seek parliamentary approval for mandatory filtering of inappropriate websites. Blocking access to a website would be authorised not by a court but by a government agency, the Australian Communications and Media Authority (ACMA).

Reporters Without Borders believes that a court should take the decision to block a website after an investigation and no government agency. The organization also believes that Internet access is a fundamental right and that the recourse of suspending a connection is a violation of the public's freedom to access information.

More recently, in a letter sent on November 15 to the Chairmen of the US Congress Committee on the Judiciary, 60 human rights groups from the international community – Reporters Without Borders among them - urged Congress to reject the Stop Online Piracy Act (SOPA), arguing that «the United States would lose its position as a global leader in

supporting a free and open Internet for public good.» (https://www.accessnow.org/policy-activism/docs. The provisions in SOPA on DNS filtering in particular will have severe consequences worldwide. In China, DNS filtering contributes to the Great Firewall that prevents citizens from accessing websites or services that have been censored by the Chinese government. By instituting this practice in the United States, SOPA sends an unequivocal message to other nations that it is acceptable to censor speech on the global Internet. SOPA would require that web services, in order to avoid complaints and lawsuits, take "deliberate actions" to prevent the possibility of infringement from taking place on their site, pressuring private companies to monitor the actions of innocent users. Wrongly accused websites would suffer immediate losses as payment systems and ad networks would be required to comply with a demand to block or cease doing business with the site pending receipt of a legal counter-notice. This domestic bill would have serious implications for international civil and human rights, which raises concerns about how the United States is approaching global internet governance.

Corporate social reponsibility

If even democratic governments have troubles to guarantee their online freedoms and promote abroad what they don't do domestically, one way of promoting online freedom is corporate social responsibility. Last month, the heads of around 40 leading technology companies in China agreed to implement government directives on online surveillance and to combat pornography, fraud and the dissemination of rumors and false information online. Industry and information technology minister Miao Wei told the Internet companies they must increase their investment in "tracking surveillance." Last October, China's restrictions on Internet use have led the US ambassador to the World Trade Organization to complain about China's "national firewall" and website blocking on the grounds that they violate WTO rules by making it harder for companies outside China to offer "services to Chinese customers."

Google has kept its promises and has stopped censuring its search engine's results in China. Google.cn users are now being redirected to their Hong Kong-based website. Despite the boldness of this move and the cold reception it received from Chinese authorities, the company managed to get its Chinese operating license renewed in the summer of 2010.

Microsoft and Yahoo! continue to practice self-censorship in China. However, Microsoft, after realizing that the fight to prevent the pirating of its software in Russia was a pretext used by the authorities to justify the seizure of computers belonging to the media and to NGOs, took measures to supply the latter with *pro bono* licences. These three U.S. companies have signed the Code of Conduct of the Global Network Initiative, a coalition of NGOs, companies and investment funds seeking to promote good practices in countries which are censoring the Net. For the first time in Egypt, companies such as Facebook, Twitter and Google have set aside their reticence and openly sided with protecting online freedom of expression. Facebook believes "no one should be denied access to the Internet." Google and Twitter set up a system to enable telephone tweeting in order to bypass net blocking in the country. YouTube made its political news channel CitizenTube available to Egyptians who want to circulate their videos. Users do not run much risk on the site and should benefit in terms of image capabilities.

In the past year – particularly during the Arab Springtime – cell phone communications have been the focus of harsher controls. In countries such as Libya and Egypt, telephone carriers have been forced to occasionally suspend their services in some locations and to transmit SMS to the population. In early February 2011, Vodafone, Mobinil and Etisalat, pressured by

the army, sent their Egyptian customers an SMS informing them of a demonstration in support of Hosni Mubarak being held that day. The headquarters of Western foreign companies apparently protested … after the fact.

There is a criminal cooperation between western hi-tech companies and authoritarian regimes. On December 1, 2011, the WikiLeaks website posted the "SpyFiles", a series of documents shedding light on the scale of the 5-billion-dollar international market in mass surveillance and interception. Around 1,100 internal documents involving 160 companies in 25 countries are being made available to the international public by WikiLeaks in partnership with five news media – *OWNI, The Washington Post, The Hindu, L'Espresso and ARD* – and a British NGO, the Bureau of Investigative Journalism.

The surveillance tools sold by these companies are used all over the world by armed forces, intelligence agencies, democratic governments and repressive regimes. The leading exporters of these technologies include the United States, France, Germany, Italy, United Kingdom and Israel. Among the companies singled out are BlueCoat (United States), Elaman (Germany), Gamma (United Kingdom), Amesys and Qosmos (France) and Aera SpA (Italy). An interactive map shows the countries and companies involved.

The equipment and software on offer constitute a vast arsenal of surveillance resources. Any computer or mobile phone can be physically located, remotely hacked, or infected with a Trojan by means of telephone surveillance tools (SMS, calls and geolocation) Internet surveillance and analysis tools (email and browsing), voice analysis and cyber-attacks.

These issues do not just concern companies in the new technologies and telecommunications sectors. PayPal's online payment service, based in the United States, decided to suspend WikiLeaks' account, claiming that its terms of use prohibit using its service "to encourage, promote, or facilitate any illegal activity." Visa and MasterCard made the same decision and suspended payments directed to the site until they have the results of internal investigations.

Recommendations to the U.S Congress to promote online freedoms

1) **Reject SOPA:** the US government can only be relevant in promoting online freedom if what it requires from its partners and/or enemies can be applicable on its own territory. SOPA is clearly a huge step back in the leader and pionneer role the United States was playing in promoting online freedom abroad.
2) **Adopt effective measures to regulate this market and to prevent the export of technology,** equipment and software to countries where they are likely to be used to violate freedom of expression and human rights.
3) **Encourage American companies to establish monitoring mechanisms** to ensure that equipment supplied to a "permitted" country is not subsequently transferred to one that is not. These regulations should also be adopted at the European Union level and by international organizations such as the Organization for Economic Cooperation and Development and the World Trade Organization.
4) **Pass the Global Online Freedom Act** that Rep. Chris Smith has been preparing and that would ban the export of these technologies to countries such as Syria and Iran that restrict online free expression and target dissidents.
5) **Encourage other countries, especially members of the OECD,** to adopt similar bills as the Gofa, to be effective worldwide and follow up with the European Union on the implementation of a European Gofa.
6) **Don't allow human rights on the side while talking about trade**: repressive behavior towards these rights are an obstacle to trade, as the U.S Ambassador to the WTO stated

last October. Therefore, these two matters should be linked in every dialogue and discussion.

7) **Request the US government to refrain from investigating supporters of Wikileaks:** last August, Jacob Appelbaum, a Seattle-based volunteer hacker for Wikileaks was interrogated at the U.S border about the website and his laptop was confiscated. The FBI is also going after Birgitta Jonsdottir, a one-time Wikileaks supporter and current member of the Icelandic parliament.

Mr. SMITH. Ms. Massimino.

STATEMENT OF MS. ELISA MASSIMINO, PRESIDENT AND CHIEF EXECUTIVE OFFICER, HUMAN RIGHTS FIRST

Ms. MASSIMINO. Thank you. Thank you, Mr. Chairman, and thank you to the subcommittee for convening this important hearing. I want to say a special thanks to you, Mr. Chairman, for your leadership on this and so many other human rights issues. You have really helped to elevate this issue of Internet freedom on the U.S. foreign policy agenda, and we are very grateful to you for your leadership.

Nearly 2 years ago when Secretary Clinton declared the freedom to connect as a fifth freedom, she cited it as an essential avenue for the exercise of fundamental human rights and said governments should not prevent people from connecting to the Internet, to Web sites, or to each other, and while she noted that these technologies are value neutral, the United States has a strong interest in ensuring a single Internet where all of humanity, she said, has equal access to knowledge and ideas. The world's information structure will become what we and others make of it, she said.

Well, today, we know that repressive states across the globe have made the Internet a dangerous place for those seeking freedom and more representative government. You, Mr. Chairman, framed the challenge that we confront today very well when you said how will all these dictatorships ever matriculate into democracy if the dissenters are all in prison, hunted down with high tech capabilities sold or acquired through U.S.-listed companies? And that is what we are here to talk about today, the role of companies.

You know, today in her speech, Secretary Clinton said that businesses have to ask themselves these questions, what should you do in a country with a history of violations of Internet freedom? How can you prevent post-purchase modifications when you sell to authoritarian regimes? Companies have to ask these questions, she said. Well, what we know now is that companies not only have to ask these questions, but they have to give informed and correct answers that reflect their own obligations to respect human rights, and so we are grateful to be able to focus today on the role of companies.

We have three primary points to make today, our observations. One, that threats to Internet freedom are proliferating, which you have already heard and know well, but that few companies have policies to address those threats; two, that the United States has an interest in ensuring that companies make the right decisions when confronted with foreign governments' demands to limit Internet services or capture private user information; and, three, stronger U.S. Government pressure, including action from the Congress is necessary to promote improved corporate policies to address the threats to Internet freedom.

I am not going to go into detail about the proliferation of threats to Internet freedom, you know them very well, and you have just heard them from the previous two witnesses, so I will move right ahead to what I would like to, what we are grappling with really at Human Rights First in working with companies who are operating in this space. Many of them, particularly surveillance and

dual-use technology providers, when you press them about their operations and what happens when their products end up in repressive countries, tend to offer a few excuses, and I think it is instructive to listen to those excuses because they provide a road map for how corporate thinking and behavior needs to change in order for companies to become partners in protecting free information and digital privacy.

So excuse number one, they say we comply with all international and national laws, what we are doing is not illegal. And at one level this is correct, obviously, but it ignores the fact that businesses have an internationally recognized responsibility to take concrete steps to protect human rights. The U.N. Guiding Principles on Business and Human Rights, which the U.N. Human Rights Council officially endorsed this year, calls for businesses to perform due diligence, to understand and avoid negative human rights impacts, that their activities or the activities of their business partners will have, and this standard is now reflected in the conflict minerals provisions of the Dodd-Frank Act in Section 1502 as well as in the OECD guidelines for multinational enterprises and the International Standards Organization's new ISO 26000, guidance on social responsibility.

And the performance standards of the International Finance Corporation. So these are not new things. There are standards out there that businesses are or should be well aware of. So for sellers of surveillance and dual-use technology or related hardware, a minimum level of due diligence would have revealed their role in the incidents that you just heard about and the role that their products could play in enabling surveillance and repression.

Excuse number two, they say, we sell to or partner with private companies, not governments, so we can't be held responsible for misuse of our product through a third party. Now, the U.N. Guiding Principles recognize that companies may be involved in human rights violations through their business relationships with third parties. An important way to protect against becoming a third-party enabler to human rights violations is to ensure that all partners in the business chain adopt policies that are consistent with the responsibility of American companies to respect human rights, so hardware companies should not sell products that could be used to violate rights to a "private" company operating in a repressive state if a reasonable amount of due diligence would show that the buyer is willing to make its technology available to government operatives. We have seen that happen time and again.

Excuse number three. They say many democracies, including the United States, have laws requiring that hardware permit monitoring of communications or allowing surveillance of online activity in order to facilitate law enforcement. The now multi-billion dollar industry for surveillance technology was born 10 years ago out of the U.S. Government's desire for better high tech tools for combating terrorism. Now we recognize that governments have an obligation to provide for security and that there are legitimate law enforcement purposes to which this technology could be put, but companies need to be sensitive to the differences in context between largely democratic and repressive or authoritarian governments. The U.S. Government certainly can step over the line sometimes,

but we have a robust, though imperfect legal and political system that can be used to curb abuses that repressive governments do not have. That means that surveillance technology in the repressive governments hence is more likely to be used in ways to violate human rights regardless of the permissible use of that technology for law enforcement purposes here in the United States. Companies need to take this into account in their decision-making, and democratic governments like the United States need to support companies to make the right decisions through appropriate export procedures and controls.

Excuse number four. The technology that we bring into undemocratic countries is a force for good that over time outweighs the human rights violations that the technology facilitates. We hear this all the time. And of course, it is undeniable that increasing the availability of technology for citizens of repressive regimes has incredible benefits for the free flow of information, for free expression, and the ability to organize and inspire others, as Mr. Payne pointed out. However, such technology is, as we are talking about today, a double-edged sword.

We recognize that the situations in these countries are complex and that the best course of action for a business is not always clear. But the first step is to ensure that American businesses do not go into these complex situations blind. If businesses gather as much information as possible regarding the society, the government, and the legal structure of the country in which they intend to operate and form a specific and comprehensive plan for dealing with the objectionable demands that government might make, they will be in a much better position not just to ask the right questions, but to give the right answers and make the right business decisions that will protect privacy and free expression.

Excuse number five. Repressive regimes are going to get this technology no matter what. If it is not from us, then it will be from a company that is based in a country with fewer restrictions. We have heard this from some countries—from some companies, and certainly in other sectors we have heard it. But in other sectors of the economy, the U.S. has never based its trade relationships on this race-to-the-bottom approach, and right now, Americans have leverage since this technology was largely developed by U.S. companies and European partners. The U.S. is in a strong position working with European allies to establish new rules to guide these transactions.

The Internet service providers also offer similar excuses, and we have similar answers to them, and I want to say that the way, I think the way forward from this, to close this gap between obligations and actual practice, there are two very important pieces which I discuss in the written testimony, and I won't go into them in detail, but one is Global Network Initiative, which you have heard about and you will hear more about, and I hope that we will talk about in the question-and-answer period, but the other really is GOFA, the legislative angle.

We are very concerned that there is a lack of pressure from the government side to help companies understand what their obligations are and to not have them navigating these dangerous waters alone. And so we applaud your efforts to push forward with this

legislation, and we hope to work together with you. We have a number of ideas that we talk about in the written statement to strengthen the legislation. We know that threats to Internet freedom today come from many places, and they come in many forms. The Obama administration has articulated quite admirably a clear policy in support of Internet freedom and has made important early progress in elaborating strategy and coordinating amongst U.S. agencies and with our allies, and the GNI is also making important progress in raising awareness of the issue among companies and in promoting wider engagement, but we know from daily press reports that the threat to Internet freedom requires a more concerted and comprehensive response from governments and the private sector. The Global Online Freedom Act addresses an important and continuing gap in existing efforts. As one of our human rights colleagues from Belarus said last year in a meeting with President Obama, "For you it is simply information, but for us, a free Internet is life." Thank you.

Mr. SMITH. Ms. Massimino, thank you very much for your testimony and your recommendations as well as providing those very useful excuses that are trotted out so routinely and then giving a very cogent response to each of them.

[The prepared statement of Ms. Massimino follows:]

TESTIMONY OF ELISA MASSIMINO
PRESIDENT AND CEO
HUMAN RIGHTS FIRST
BEFORE THE HOUSE FOREIGN AFFAIRS SUBCOMMITTEE ON AFRICA, GLOBAL HEALTH AND HUMAN RIGHTS
"PROMOTING GLOBAL INTERNET FREEDOM"
DECEMBER 8, 2011

Introduction

Chairman Smith and Members of the Subcommittee, thank you for convening this hearing to examine threats to global internet freedom. I appreciate the opportunity to be here this afternoon to share Human Rights First's perspective on this critical issue and to discuss ways that we can work together with you to advance human rights protections. Your leadership, Chairman Smith, has helped to elevate Internet freedom on the U.S. human rights and foreign policy agenda. We look forward to continuing to work with you to assist in these efforts.

Nearly two years ago, Secretary of State Hillary Clinton boldly declared "the freedom to connect" as an essential avenue for the exercise of fundamental human rights, saying that "governments should not prevent people from connecting to the Internet, to websites or to each other." She noted that, while technologies are value neutral, the United States has a strong interest in ensuring "a single Internet where all of humanity has equal access to knowledge and ideas." "[T]he world's information structure," she said, "will become what we and others make of it."

Unfortunately, repressive states across the globe have made the Internet a dangerous place for those seeking freedom and more representative government. Chairman Smith framed the challenge we confront today: "How will all these dictatorships ever matriculate into democracy if the dissenters...are all in prison, hunted down with high-tech capabilities sold or acquired through U.S.-listed companies?" The answer lies in Secretary Clinton's challenge: "We need to synchronize our technological progress with our principles." As she explained, "this issue isn't just about information freedom… it's about whether we live on a planet with one Internet, one global community, and a common body of knowledge that benefits and unites us all, or a fragmented planet in which access to information and opportunity is dependent on where you live and the whims of censors."

For the U.S. government, meeting this challenge means aligning American principles, economic goals and strategic priorities. For companies, as the Secretary noted, "This issue is about more than claiming the moral high ground. It really comes down to the trust between firms and their customers…. People want to believe that what they put on

the Internet is not going to be used against them."

Today's hearing examines the role of U.S. companies in managing user information in countries that maintain repressive policies, and possible U.S. policy responses to promote global internet freedom. Human Rights First offers three main observations:

1. Threats to internet freedom are proliferating, but few companies have policies to address these threats.

2. The United States has an interest in ensuring that companies make the right decisions when confronted with foreign government demands to limit internet services or capture private user information.

3. Stronger U.S. government pressure, including congressional action, is necessary to promote improved corporate policies to address threats to internet freedom.

I. Threats to Internet Freedom are Proliferating

When this Subcommittee first began discussing legislation to address threats to internet freedom, much of the attention was focused on China and its Great Firewall. American companies including Cisco, Yahoo, Microsoft and Google have faced criticism for cooperating with China in ways that further repressive internet policies. This year, Cisco was sued in the United States for seeking contracts with the Chinese government. The lawsuits allege Cisco knew that its services and products would be used by Chinese law enforcement entities for censorship and surveillance. Just this past summer, there were reports that Cisco and Hewlett Packard were bidding on a contract to install as many as 500,000 cameras in a single Chinese city. Cisco has denied the reports.

The threats to global internet freedom are not limited to the Chinese model. The Arab Spring raises fresh challenges, including the role of U.S. hardware and equipment companies in facilitating surveillance and repression, and the policies of telecommunications companies facing government requests to shut down.

In the Middle East, where the United States is actively supporting pro-democracy activists, we know firsthand that activists use the Internet at their peril. In Egypt, the ruling military regime has expanded existing emergency laws to more tightly control all forms of communication. Prominent bloggers have been arrested and face trial in military courts. The surveillance blanket that former Egyptian President Hosni Mubarak used to target dissidents remains in place. And we now know that Egypt was not alone in surveilling its citizens. As *Bloomberg Markets*, the *Wall Street Journal*, and the *Washington Post* have reported, American and European companies helped to create and maintain surveillance webs throughout the Middle East. The capabilities include real-time surveillance of millions of people and precision filtering of the Internet.

In Syria, where more than 4000 people have been killed since March, the Assad regime's surveillance system includes products from the California-based technology companies NetApp and Blue Coat Systems. These companies have been quick to say that they have

not violated any U.S. or international law, and they are right. Although the U.S. government has unequivocally condemned the brutal tactics used by Syria, Iran, Egypt, Libya, and others, and has passed strong sanctions barring the sale of certain products into those countries, the technologies at issue here are not restricted.

NetApp, a California company that makes storage hardware and software to archive emails, sold its product to an Italian company. NetApp apparently took no further steps to determine how its equipment would be used, or who the end user would be, before contracting with the Italian company. The Italian company installed that technology, along with products from various other U.S. and European companies, in Syria. Syria's security forces used the technology to target and arrest activists and used the information it obtained to target people for torture. The Syrian government similarly used technology from Blue Coat Systems, another California-based company that makes web security products capable of monitoring and blocking web traffic. Blue Coat claims to have sold the technology to Dubai, believing they were destined for a department of the Iraqi government. Executives claim to have no idea how the product made its way into Syria, but the Commerce Department is now investigating Blue Coat's role.

II. Ensuring that Companies Understand and Take into Account Human Rights Risks, and Make the Right Decisions

Surveillance and Dual-Use Technology Providers

When pressed, companies that sell surveillance and dual-use technology that ends up being used for persecution and repression tend to offer several excuses. These excuses provide a roadmap for how corporate thinking and behavior needs to change in order for companies to become partners in protecting freedom of information and digital privacy.

Excuse #1: "We comply with all international and national laws. What we are doing isn't illegal."

At one level this is correct, but it ignores the fact that businesses have an internationally-recognized responsibility to take concrete steps to protect human rights. The UN Guiding Principles on Business and Human Rights, which the UN Human Rights Council officially endorsed this year, calls for businesses to perform due diligence to understand and avoid any negative human rights impact that their activities, or the activities of their partners, will have. This standard is now reflected in the conflict minerals provisions of the Dodd-Frank Act (Section 1502 requires companies using conflict minerals to report to the SEC on whether such minerals originated in the Democratic Republic of Congo), as well as in the OECD Guidelines for Multinational Enterprises (recommendations for responsible business conduct from the 42 OECD adhering governments, accounting for 85% of foreign direct investment), the International Standards Organization's new ISO 26000 guidance on social responsibility (which provides harmonized guidance for private and public sector organizations based on international consensus and is aimed at promoting implementation of best practices), and the performance standards of the International Finance Corporation (requirements for borrowers, principally corporations and States, to qualify for project funding.)

For sellers of surveillance and dual-use technology or related hardware, a minimal level of due diligence would have revealed the role their products could play in enabling surveillance and repression by authoritarian Middle Eastern governments.

Excuse #2: "We sell to or partner with private companies, not governments, so we can't be held responsible for misuse of our product through a third party."

The UN Guiding Principles recognize that companies may be involved in human rights violations through their business relationships with third parties. An important way to protect against becoming a third party to human rights violations is to ensure that all partners in the business chain adopt policies that are consistent with the responsibility of American companies to respect human rights.

Hardware companies should not sell products that could be used to violate rights to a "private" company operating in a repressive state if a reasonable amount of due diligence would show that the buyer is willing to make its technology available to government operatives. This was the case when Adaptive Mobile, an Irish company, sold monitoring and filtering technology to Irancell, Iran's second-largest private mobile service provider. Reasonable due diligence would have revealed that Irancell makes its technology available for use by Iran's security forces, who have a long, well-documented history of tracking political dissidents and violently silencing them. American companies could as easily become complicit in an arrangement between a "private" company and a repressive regime if they do not take the steps to educate themselves about the risks and demand that business partners adopt human rights policies commensurate with American obligations.

Excuse #3: "Many democracies—including the United States—have laws requiring that hardware permit monitoring of communications, or allowing surveillance of online activity, in order to facilitate law enforcement."

The now multi-billion dollar industry for surveillance technology was born ten years ago out of the U.S. government's desire for better high-tech tools for combating terrorism. Human Rights First recognizes that governments have the obligation to provide for security and there are legitimate law enforcement purposes to which this technology can be put. But companies need to be sensitive to the differences in context between largely democratic and repressive or authoritarian ones. The United States government can step over the line but we have robust, though imperfect, legal and political systems that can be used to curb abuses facilitated by such technology. Repressive regimes do not, and there is no check on their authority. That means that surveillance technology in the hands of repressive governments is much more likely to be used in ways that violate human rights, regardless of the permissible use of that technology for law enforcement purposes. Companies need to take this into account in their decision-making. And democratic governments need to support companies to make the right decisions through appropriate export procedures and controls.

Excuse #4: "The technology that we bring into undemocratic countries is a force for good that, over time, outweighs the human rights violations that the technology facilitates."

It is undeniable that increasing the availability of technology for citizens of repressive regimes has incredible benefits for the free flow of information, freedom of expression, and the ability to organize and inspire others. However, such technology is a double-edged sword, equally capable of suppressing free expression and silencing dissenters. Human Rights First recognizes that the situations in these countries are complex, and that the best course of action for a business is not always clear. The first step, though, is to ensure that American businesses do not go into these complex situations blind. If businesses gather as much information as possible regarding the society, government, and legal structure of the country in which they intend to operate, and form a specific, comprehensive plan for dealing with the objectionable demands that a government might make, they will be in a much better position to protect free expression and privacy to the greatest possible extent.

Excuse #5: "Repressive regimes are going to get the technology no matter what – if not from us, then from a company based in a country with fewer restrictions."

Some companies have claimed that if *they* don't sell this technology, the Chinese will. But in other sectors of the economy, the United States has never based its trade relationships on "race to the bottom" rules. And right now Americans have leverage, since this technology was largely developed by U.S. companies and European partners. The United States is in a strong position, working with European allies, to establish new rules to guide these transactions.

Internet Service Providers

Internet service providers operating in repressive country environments face similar human rights challenges in that they can be used – wittingly or not – to facilitate abuses. Companies in this situation offer excuses similar to those offered by surveillance and dual-use technology companies, and they are no less problematic.

Excuse #1: "We are required to follow the laws of the jurisdictions where we operate."

For internet service providers, where national laws may require censorship in conflict with international human rights protections, companies have an obligation to honor the spirit of international standards without violating national law. They can honor the spirit of their responsibility to respect human rights by pushing back as much as legally possible against the dictates of repressive regimes. Google's decision to stop censorship by providing a link to its uncensored Hong Kong site illustrates this principle, and provides a useful example for other ISPs to follow. Companies can also: request that government demands be narrowly framed and based on judicial process; challenge demands that do not meet these criteria; be transparent with users about how they manage their requests; and work collectively with other companies and their home government to promote more open and rights-respecting policies.

Excuse #2: "We partner with host country service providers to obtain entry to new markets and don't have control over their policies."

U.S. service providers, such as search engines and social networking sites, are

increasingly seeking to expand into new markets. Often the easiest way to do this is to partner with local providers. Facebook, which has been banned in China, is in talks with China's leading search engine Baidu to launch a new social network inside China. Baidu is a censored platform. There are concerns that Facebook's China service would comply with China's extensive censorship laws, which will only serve to reinforce the hold that China's Great Firewall has over its citizens. Consistent with the UN Guiding Principles, Facebook should assess the risks of partnering with Baidu and develop policies to prevent or minimize the impact of China's censorship and surveillance laws and practices. This could include pressing Baidu to adopt counterpart policies and establishing in country capacity to assist users in novel and safe uses of the platform. Facebook is well aware of the potential risks to human rights and needs to address these underlying issues early and institute benchmarks to gauge progress. This could include ongoing risk monitoring and review along with stakeholder engagement. Facebook also needs to explain to users, in clear and accessible terms, what personal information is being gathered, under what circumstances it is shared, and how such information can best be managed by users to limit unintended disclosure. Within the limits of Chinese law, Facebook should also strive to explain to users how it is handling specific government requests for information. Potential investors in Facebook's anticipated IPO should be asking the company how it intends to address these very real business and reputational risks.

In sum, when faced with situations where business operations carry serious risks of facilitating human rights violations, we expect companies to do the following:

Conduct a risk assessment. Identify where company operations might affect freedom of expression and privacy rights of users.

- Develop policies to address the risks, obtain approval by senior management, and ensure the policies are understood and implemented company-wide.
- Know your partner, distributor, customer, and other business partners and ensure that they have similar policies to identify and address risks.
- Obtain outside, independent evaluation of company performance, and publicly report those results.

III. Closing the Gap between Company Human Rights Obligations and Actual Practices

Human Rights First's work on internet freedom has found a substantial gap between the human rights obligations of ICT companies and actual practices to minimize the human rights risks. In the ICT sector, different companies have different business models and, as a result, different concerns and approaches to human rights risks. However, each of them has potential human rights impacts, and will put their businesses and reputations at risk if they do not take affirmative steps to address those impacts in a credible and transparent way. External pressure is vitally needed to help companies recognize this responsibility and close the accountability gap.

The Global Network Initiative

Five years ago, the issue of internet freedom was not on anyone's agenda. Strong Congressional leadership from this Subcommittee and others forced internet service providers doing or considering doing business in repressive countries to sit up and take notice. In response, Google, Microsoft and Yahoo joined with other interested stakeholders – including Human Rights First – to create a voluntary multistakeholder initiative to address these concerns. The Global Network Initiative recognizes that companies face a human rights challenge and a choice. The GNI's members endorse a set of Principles on freedom of expression and privacy grounded in international human rights norms. The company members also commit to a set of implementation guidelines, to translate principles into policies and practices, and to submit to independent external assessments of their performance.

Human Rights First believes that voluntary multistakeholder initiatives can play a valuable role in addressing the human rights impacts of global corporate operations. Whether or not they succeed, however, depends on whether they can demonstrate a positive impact on the human rights at issue. We joined GNI to press companies not just to commit to core principles, but also to act responsibly. We ask companies to take a more assertive stand, individually and collectively, to challenge intrusive practices by governments that mute dissent and persecute individuals who speak out against government policies and practices. We expect GNI to be in a position to show that membership makes a meaningful difference in addressing threats to freedom of expression and privacy online.

Mr. Chairman, we have a long way to go. To date, the GNI has sparked lots of discussion among companies, but the initiative's effectiveness in addressing concerns about freedom of expression and privacy has not yet been established. For Human Rights First, GNI's effectiveness will depend on the extent to which company assertions about what they have done to implement GNI Principles to advance freedom of expression and privacy can be verified through transparent reporting and independent monitoring and evaluation. This assessment can help to identify both best practices and where companies are falling short. It can also help us to better understand the limits of collective voluntary action, and areas where the U.S. and like-minded governments need to reinforce – with legislation or regulation if necessary – both the expectations of companies, including policies and reporting, and of host governments to adopt rights respecting policies. In this regard, there is an important role for Congress to play in continuing to highlight expectations of companies and to press for adoption of responsible policies. The lack of focused pressure has given ICT companies the time and space to stall on accountability.

The Global Online Freedom Act

In order to ensure that U.S. policies are aligned to advance more responsible government and corporate behavior, the GOFA bill is an important milestone, and HRF supports the overall objectives. We agree that the U.S. government can do a better job of identifying

and reporting internet-restrictive policies, and that this should be done across all countries. Such reporting will also permit better coordination of U.S. trade and diplomatic efforts. We also agree that private companies should have transparent policies to address government demands to censor content, surveil users, or to provide private user information. And we strongly support efforts to identify and curb hardware equipment sales to repressive regimes.

We understand that the bill is under discussion and look forward to working with you to strengthen it and ensure prompt passage. At this preliminary stage, we offer a few general observations on key provisions.

Greater Integration of U.S. Government Human Rights and Trade Policies

Section 103 requires that State Department annual country human rights reports include assessments of restrictions on online speech and privacy. Section 104 requires that State, based on these assessments, designate specific countries as "internet restricting countries" where a pattern of substantial restrictions on internet freedom exists. We believe this overall approach is useful, and will facilitate better coordination of U.S. policy initiatives. Today's announcement of a multigovernmental contact group to coordinate policy and assistance is welcome news. The reporting provisions of GOFA should help enhance U.S. effectiveness and leadership in seeking global consensus and more uniform and rights-respecting approaches to internet freedom policies.

Section 105 requires the U.S. Trade Representative to report on trade related disputes arising from "government censorship or disruption of the internet." The provision also states the Sense of Congress that the United States pursue complementary trade policies that ensure the free flow of information. Human Rights First believes that human rights and trade policy approaches to internet freedom are currently not well harmonized, and agree that they should be integrated if they are to be effective in ensuring one global internet, where all citizens have access to the same content. We recommend that this provision be broadened to require USTR reporting on the full range of potential trade restricting conduct by governments that affect this sector, including conditions on market access or licensing, technical requirements aimed at enabling surveillance – and any government sponsored or condoned hacking of sites, restrictions on advertising, and selective enforcement of intellectual property rights. We would go further and require that the annual National Trade Estimates reports include an analysis of country policies with implications for the free flow of information online and the privacy of user data.

As the Subcommittee is aware, there is an ongoing and lively debate about proposals to address the adequacy of current laws to protect the rights of content holders against online piracy. The House bill, H.R. 3261, the Stop Online Piracy Act, would end the existing and limited protections for internet intermediaries against liability for piracy of third party content. While we recognize the need to protect against piracy, this approach raises the specter of censorship and disruption of the free flow of information on the global internet because the language is overbroad, there is a complete lack of due process built in, and the provisions too closely resemble the censorship approaches taken by

repressive regimes, giving those regimes cover for their harmful policies. In so doing, SOPA damages U.S. credibility on global internet freedom. Civil liberties and human rights organizations—as well as a growing number of ICT companies--have urged that antipiracy proposals focus on financial intermediaries rather than internet hosts. Rep. Darrell Issa, in collaboration with Sen. Ron Wyden, is working on such an approach to address these concerns.

Corporate Accountability for Online Freedom

Section 201 requires internet companies subject to SEC reporting requirements and operating in internet restricting countries to disclose their (1) human rights due diligence policies, (2)polices regarding the collection and disclosure of personally identifiable information, and (3) for search engines and content hosts, steps to advise users of any restrictions on online content. This provision is an important step forward in promoting corporate transparency and accountability.

The concept of human rights due diligence is now widely understood to include four central elements: a human rights risk assessment, a policy grounded in international human rights norms, senior management level engagement and company-wide implementation, and an independent external assessment and report to the public. These four elements, part of the Guiding Principles, are the foundation of a responsible corporate approach to online freedom of expression and privacy risks.

Section 201, by reference to the OECD Guidelines, should properly be read to include these elements. For the sake of clarity, we recommend that it closely mirror the language of the Guiding Principles and reference them as a baseline.

In fact, several of Section 201's requirements are embedded in privacy orders between the FTC and three companies that would be covered by Section 201 – Google, Twitter and, most recently, Facebook. These orders require the adoption of specific privacy policies to address user concerns about disclosure – for both existing and new products or features, and regular independent external reviews. While we have some questions about the scope of the Facebook order and the way in which it will be implemented, we believe the order, and a similar order covering Google and Twitter, is a step toward the goal of companies implementation of robust due diligence. We encourage the subcommittee to maintain oversight of the implementation of these orders to ensure these orders advance that goal.

Export Controls

Section 301 would require export licenses for the sale of technology that can be used for censorship of surveillance by internet-restricting countries. This important and timely provision would help to address an obvious gap in existing law that has enabled the sale of such equipment to authoritarian regimes and their use in suppressing dissent. We recommend that the coverage of **Section 201** be expanded to include these companies whose products and services may post human rights risks in the hands of internet-

restricting companies. As we noted earlier, companies in this sector need to do a better job of identifying and addressing risk, including risks stemming from sales to or through partners, distributors, suppliers and other third parties.

The subcommittee should maintain active oversight of this issue to assess efficacy of current approaches and the need for additional measures.

Conclusion

Threats to internet freedom now come in many forms, from many places. The Obama Administration has articulated a clear policy in support of internet freedom and has made important early progress in elaborating its strategy, coordinating among US agencies and with our allies, and extending support to netizens under threat. The GNI is also making progress in raising awareness of the issue among companies and in promoting wider engagement. But we know from daily press reports that the threats to internet freedom require a more concerted and comprehensive response, from government and the private sector. The proposed legislation addresses an important and continuing gap in existing efforts. As one of our human rights colleagues from Belarus said last year in a meeting with President Obama, "for you, it's simply information, but for us [a free internet] is life."

Mr. SMITH. Ms. MacKinnon.

STATEMENT OF MS. REBECCA MACKINNON, BERNARD L. SCHWARTZ FELLOW, THE NEW AMERICA FOUNDATION

Ms. MACKINNON. Thank you very much, Mr. Chairman, and Ranking Member Payne for the opportunity to testify today and for your leadership on this issue. I look forward to answering your questions after our opening statements.

In my testimony today, I am going to touch upon the lessons learned from the Arab Spring, and particularly the role of companies in suppressing dissent in the Middle East and North Africa as well as in China and elsewhere. More details can be found in my written testimony. I will then conclude with recommendations.

After Egyptian President Hosni Mubarak stepped down in February, Google executive and Facebook activist Wael Ghonim famously declared, "If you want to liberate a society, just give them the Internet." Sadly, events since then, as detailed by previous testimony here today, have proven that Internet access alone is insufficient in the face of aggressive surveillance, cyber attacks, and brutal physical reprisals against cyber dissidents.

In the Internet age, citizens' ability to organize, express dissent, and conduct political discourse depends increasingly on technologies that are created and often operated by companies. The unholy alliance of unaccountable government and unaccountable and amoral business is thus one of the most insidious threats to democracy everywhere. As I explain in my written testimony and have described in previous hearings, China is the most extreme example of how the public-private partnership in digital repression can work, but variants and permutations of such partnerships are exclusive neither to China nor to entirely authoritarian regimes.

I, therefore, recommend the following: First, we need to improve and update export control laws, make collaboration with repression more difficult, require companies selling surveillance technologies overseas to conduct due diligence about the context in which these products are likely to be used and the human rights implications, require transparency in what is sold to whom and where it is used, with reporting requirements for companies as well as for U.S. Government agencies approving sales and exports. Export laws should also be revised and updated so that activists in countries like Syria are not denied access to communication tools by Internet companies fearful of violating sanctions.

Second, we need to require corporate accountability and transparency in all markets. Companies should be required to report on how they gather and retain user information, how they share that information with governments, as well as the volume and nature of requests made by governments to delete or block user content or hand over user information. Mandating greater accountability and transparency on the part of corporations as well as on the part of governments about their access to corporate data and the demands they are making, and about how citizens communications are censored or monitored can promote consumer awareness and stimulate demand for services that people can associate with respect for their rights and stimulate lack of demand for companies that are not respecting people's rights. Shareholders and investors must

also be properly informed about what they are supporting so that they can make investment decisions based not only on financials, but also on what kind of world these companies are helping to create.

Third, the support of multi-stakeholder corporate accountability and assessment efforts is important. All information and communications technology companies must not only accept human rights risks and responsibilities, which they clearly hold, as we have heard today, they must conduct human rights due diligence, but they must also be required to undergo independent assessment to determine whether they are living up to their claims. The Global Network Initiative's globally applicable principles on free expression and privacy were developed over several years in a multi-stakeholder process involving not only companies but also human rights groups, socially responsible investors, and academic experts. They are supported by implementation guidelines and an accountability framework that applies to all markets and can be adapted to a range of business models, including hardware companies and Internet service providers. Companies that choose not to engage with the GNI should be required to submit to some other multi-stakeholder assurance process of at least equal if not greater rigor and independence.

And finally, we need to make sure that all U.S. legislation is compatible with global Internet freedom. All bills involving Internet regulation, from cyber security to copyright protection, to other challenges the Internet has wrought should undergo their own human rights assessments before introduction to identify potential, unintended consequences for human rights, free expression, and global Internet freedom. The Stop Online Piracy Act and the Protect IP Act, now before the House and Senate, are examples of bills that would have benefited greatly from human rights due diligence and due diligence about their impact on global Internet freedom before seeking remedies to address copyright infringement, which unfortunately would inflict collateral damage on free expression by effectively establishing a nationwide filtering system and blacklisting system as well as legal liabilities for Internet companies that would compel Web site owners to proactively monitor and censor users in ways that are not unlike the ways in which Chinese companies are required to monitor and censor.

In short, there is no silver bullet solution for Internet freedom any more than there has ever been a silver bullet solution for freedom in the physical world. As in the offline world, protecting human rights in the digital realm requires public awareness, vigilance, and constant involvement as well as an ecosystem of industry, government, and concerned citizens working together with a shared commitment to basic rights and values. Thank you very much.

Mr. SMITH. Thank you very much for your very, very extensive recommendations, past and present.

[The prepared statement of Ms. MacKinnon follows:]

Testimony of
Rebecca MacKinnon
Bernard L. Schwartz Senior Fellow, New America Foundation
Co-Founder, Global Voices Online (globalvoicesonline.org)

At the hearing:
"Promoting Global Internet Freedom"

United States House of Representatives
Committee on Foreign Affairs
Subcommittee on Africa, Global Health, and Human Rights
Thursday, December 8, 2011

Thank you, Mr. Chairman and ranking member Payne, for the opportunity to testify today. I am Rebecca MacKinnon, a Bernard L. Schwartz Senior Fellow at the New America Foundation. Earlier in my career I worked as a journalist for CNN in China for more than nine years. Since 2004 while based at several different academic institutions I have studied Chinese Internet censorship alongside global censorship and surveillance trends, examining in particular the role of the private sector. In 2006 I became involved in discussions between members of industry, human rights groups, investors, and academics which eventually led to the launch in 2008 of the Global Network Initiative, the multi-stakeholder initiative that aims to help Internet and telecommunications companies uphold the principles of free expression and privacy around the world. Seven years ago I also co-founded an international citizen media network called Global Voices Online, with bloggers and activists contributing from more than 100 countries. Several of our community members have been jailed or exiled because of their online activities, and many more have been threatened.

Based on my research as well as my practical experience working with bloggers and activists around the world, my forthcoming book, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* argues that the very aspects of the Internet that empower activism and dissent are under threat. Citizens everywhere increasingly depend on the Internet and mobile technologies for political and civic discourse, along with so many other aspects of our lives. Without a robust global movement – and genuine commitment by governments and companies – to keep the Internet open and free, I am concerned that the Internet will grow increasingly inhospitable to democratic discourse and dissent.

I will begin my testimony with some of the lessons learned from the Arab Spring about the challenges to Internet freedom worldwide – by activists and Internet freedom supporters as well as by authoritarian regimes. I will then address some of the inconvenient truths about American companies, American investors, and United States policy and conclude with policy recommendations.

Lessons of the Arab Spring

After Egyptian President Hosni Mubarak stepped down earlier this year, Google executive and Facebook activist Wael Ghonim famously declared: "If you want to liberate a society just give them the Internet." Unfortunately, events of the past year have shown that Internet access alone – even relatively uncensored access – is insufficient in the face of aggressive surveillance, especially when combined with other tactics such as cyber-attacks against activists' online accounts and websites, plus physical reprisals against prominent cyber-dissidents.

Until recently, Congressional efforts to support Internet freedom have focused most energetically on supporting the development and dissemination of circumvention technologies that help Internet users gain access to censored websites.[1] While those technologies continue to be useful for many activists around the world, most of them are no match for the cutting-edge surveillance technology developed largely by American and European companies now for sale around the world, as several of the other witnesses today have described in detail. Technically speaking, simple circumvention tools such as basic virtual private networks (VPN's) are quite easy to set up. The ease of setup for a particular tool, however, means it is likely to be just as easy for someone to block, monitor, and control that tool. In fact, circumvention tools that are marketed primarily to activists and whose security practices fail to keep up with the constant innovations of state-of-the-art Western products can even increase activists' vulnerability to surveillance, even as they successfully evade censorship.[2]

Insufficient attention has been devoted to the urgent need to revise export control laws, which not only fail to prevent the sale of surveillance technology that is used by many repressive regimes, but inadvertently deprive activists in countries like Syria to the tools and international connections that would help them succeed. Most infamously, surveillance products manufactured by the American company Blue Coat have found their way to Syria and Burma.[3] Meanwhile activists have struggled to gain access to basic communication tools – like Skype - that companies fearful of violating sanctions have blocked them from using. In August, the Treasury Department's Office of Foreign Assets Control (OFAC) issued a general license allowing the export of "certain services incident to Internet-based communications." It specifically notes that transactions related to the exchange of personal Internet communications like instant messaging, chat and email, social networking, photo- and video-sharing, web browsing, and blogging are permitted.[4]

But as the Electronic Frontier Foundation's Jillian York points out the problems for activists have not ended there. "Restrictions from the Department of Commerce's Bureau

---

[1] http://lugar.senate.gov/record.cfm?id=331192

[2] https://www.torproject.org/press/presskit/2010-09-16-circumvention-features.pdf and http://www.guardian.co.uk/technology/2010/sep/17/haystack-software-security-concerns

[3] http://www.washingtonpost.com/world/national-security/us-probes-use-of-surveillance-technology-in-syria/2011/11/17/gIQAS1iEVN_story.html http://citizenlab.org/2011/11/behind-blue-coat/ and http://citizenlab.org/2011/11/behind-blue-coat-an-update-from-burma/

[4] www.treasury.gov/resource-center/sanctions/Programs/Documents/syria_gl5.pdf

of Industry and Security (BIS) still appear to prevent communications tools and services from being exported to Syrians without a license," she writes. "We think that because of these restrictions, Syrians still cannot access Google products Chrome and Earth, cannot download Java, among various other tools, and cannot use hosting services like Rackspace, SuperGreenHosting and others."[5]

While export control law clearly needs revision in order to match realities on the ground, the broader problem is the result of failure by most Western technology companies – many of them American – as well as most of their investors, to accept responsibility for the human rights implications of their businesses, or to make meaningful efforts to acknowledge let alone mitigate the human rights risks of their technologies. As Jerry Lucas, president of TeleStrategies Inc., operator of the Intelligence Support Systems (ISS) World Americas conference, an annual trade show for makers of surveillance technology recently told the *Wall Street Journal*: "We don't really get into asking, 'Is this in the public interest?'"[6]

Mr. Chairman, your leadership on this issue and your continued efforts to hold companies accountable for their actions is vital not only to activists fighting repressive regimes but to Americans who believe that it is unacceptable for businesses based in the United States and supported by American investors to participate in the suppression of the very kinds of civil liberties and human rights protections that people around the world are risking their lives for - and which we continue to fight to preserve here at home.

The China Model: Public-Private Partnership in Repression

In the Internet age, citizens' relationship with government, and their ability to conduct political debate and discourse, increasingly depends on technologies that are created, owned and operated by companies. Because of this dependence, the unholy alliance of unaccountable government with unaccountable and amoral business is one of the most insidious threats to democracy everywhere.

In the wake of the Arab Spring as well as a number of domestic incidents that activists have seized on to criticize government corruption and abuse, the Chinese government has increased its pressure on Internet companies to improve their internal censorship and surveillance systems, citing the danger of "online rumors" and holding companies responsible for stopping their spread.[7] Sina Weibo, China's most popular Twitter-like microblogging service, is believed to employ approximately 1,000 people to monitor and censor users. The CEO of Tencent, another Internet company, has said publicly that his company is working to develop new technologies and methods to better censor and monitor users.[8] Many of the largest Chinese Internet companies, including Sina,

[5] https://www.eff.org/deeplinks/2011/09/stop-the-piecemeal-export-approach
[6] http://online.wsj.com/article/SB10001424052970203611404577044192607407780.html
[7] http://digicha.com/index.php/2011/12/attack-creators-and-propagators-of-internet-rumors-head-on-a-new-china-internet-campaign-starting/
[8] http://online.wsj.com/article/SB10001424052970204394804577009100441486814.html

Tencent, and Baidu (China's largest search engine) are listed on US stock exchanges and many more are beneficiaries of copious private American investment.

As I described in testimony to this committee in March of last year, China leads the world when it comes to institutionalizing and codifying the public-private partnership in digital repression. China's system of blocking or filtering overseas websites is merely the first level of the Chinese Internet control system. When it comes to websites and Internet services over which Chinese authorities have legal jurisdiction, 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.[9] All Internet companies operating within Chinese jurisdiction – domestic or foreign – are held liable for everything appearing on their search engines, blogging platforms, and social networking services. They are also legally responsible for everything their users discuss or organize through chat clients and messaging services. In this way, much of the censorship and surveillance work is delegated and outsourced by the government to the private sector – who, if they fail to censor and monitor their users to the government's satisfaction, will lose their business license and be forced to shut down. It is also the mechanism through which China-based companies must monitor and censor the conversations of more than fifty million Chinese bloggers. Politically sensitive postings are deleted or blocked from being published. Bloggers who become too influential in the wrong ways can have their accounts shut down and their entire blogs erased. Much of the front-line digital surveillance work is conducted not by "Internet police" but by employees of Internet and telecommunications companies, who then cooperate closely with authorities.[10]

Efforts to increase corporate accountability and transparency

In the absence of meaningful legislation addressing pressure by governments on companies to conduct surveillance and censorship in a manner that violates internationally recognized norms on free expression and human rights, in 2008 a group of companies, socially responsible investors, human rights groups and academic experts

---

[9] See *Race To the Bottom: Corporate Complicity in Chinese Internet Censorship* by Human Rights Watch (August 2006), at http://www.hrw.org/reports/2006/china0806/. Also "Search Monitor Project: Toward a Measure of Transparency," by Nart Villeneuve, Citizen Lab Occasional Paper, No.1, University of Toronto (June 2008) at http://www.citizenlab.org/papers/searchmonitor.pdf

[10] 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

launched the Global Network Initiative on whose board of directors I currently sit along with Elisa Massimino of Human Rights First who is also testifying at this hearing.[11]

Just as companies have a social responsibility not to pollute our air and water or exploit twelve-year-olds, companies have a responsibility not to collaborate with the suppression of peaceful speech. The GNI's philosophy is grounded in the belief that people in all markets stand to benefit from Internet and mobile technologies. In most cases companies can contribute to economic prosperity and individual empowerment by being engaged in countries whose governments fail to uphold their human rights obligations– as long as they are aware of the human rights implications of their business and technical decisions. It is reasonable to expect all companies in the ICT sector to include human rights risk assessments in their decisions about market entry and product development, just as they and other companies consider environmental risks and labor concerns.

With a multi-stakeholder membership including human rights groups, socially responsible investors and academics such as myself, the GNI's goal is to help companies minimize their potential complicity in human rights abuses while bringing expanded Internet communications and mobile access to the people who stand to benefit most from these technologies. All GNI members are participating in this process because they believe in the transformative importance of the ICT sector and want innovative businesses to be successful and competitive. We are working with companies in good faith. GNI member companies recognize that they face difficult problems, and that they could use support and advice in order to assess risks and avoid mistakes. When mistakes do happen, companies should be held appropriately accountable in ways that can help the entire industry learn from these mistakes and do a better job of avoiding them in the future.

While the GNI's current membership includes only five companies, Yahoo, Google, Microsoft, Evoca and Websense, its globally-applicable principles on free expression and privacy are supported by implementation guidelines and an accountability framework that can be adapted to a range of business models, including hardware companies and Internet service providers, if these companies choose to engage with the GNI. The GNI is in active discussions with a number of companies and are hopeful that more will join in the near future. Legislation is clearly needed to deal with companies that demonstrate time and again that they have no interest in human rights. But for companies that recognize the human rights implications of their businesses, the GNI currently is the only institution in the world today that provides any sort of operational policy framework, vigorous stakeholder engagement, and an independent assurance process which organizations like Human Rights Watch and Human Rights First would not have associated themselves if they did not believe it to be meaningful, despite their concerns that its effectiveness remains to be proven.

Indeed, the GNI has yet to prove itself with so few companies on board and the first

[11] http://globalnetworkinitiative.org

round of assessment still underway, to be completed in January and the results announced some time early next year. Joining GNI will not turn companies into saints and it will not prevent all problems. It is a floor not a ceiling: setting the most basic common standards - below which a company that wants to be considered socially responsible should work hard not to fall. If most Internet and telecommunications companies cannot even reach what many people in the human rights community consider to be a low bar, that does not bode well for the future of human rights and civil liberties in the Internet age. Something must be done.

The bottom line is that all companies in the information technology sector have an obligation to recognize their human rights risks and responsibilities. As Ronald Reagan once said, after a commitment is made: "trust, but verify." Reporting must be accompanied by credible verification. Those who choose not to engage with the GNI should be required to find other appropriate policy and operational responses to address the inescapable human rights implications of their products or services. However, based on my own experience with the years of negotiations surrounding GNI's formation, I can attest to how difficult it will be for other alternative organizations to match GNI's processes not only in terms of operational utility but also transparency, accountability, and stakeholder engagement.

Inconvenient Truths

In October this year, the U.S. Trade Representative Ron Kirk sent a letter to the Chinese government requesting information about its censorship practices.[12] Foreign ministry spokeswoman Jiang Yu brushed off his query with a comment that Chinese censorship follows "international practice."[13] Her response was specious given that China operates the world's most elaborate and opaque system of Internet censorship in the world. Yet human rights activists around the globe are concerned that legislative trends in the U.S. and other democracies are emboldening their own governments to construct opaque and accountable public-private partnerships in censorship and surveillance.

Last year when the Egyptian activist Alaa Abd El Fattah – who spent time in jail under Mubarak and is currently back in jail under the transitional military government – was asked to suggest what democratic nations can do to help cyber-activists in the Middle East and North Africa, he called on the world's democracies to "fight the troubling trends emerging in your own backyards" which "give our own regimes great excuses for their own actions."[14]

As the United States advocates Internet freedom around the world, the inconvenient reality is that over the past decade, beginning with the Patriot Act, laws have been passed and policies implemented that make it vastly easier for government agencies to track and

[12] http://www.ustr.gov/about-us/press-office/press-releases/2011/october/united-states-seeks-detailed-information-china%E2%80%99s-i

[13] http://www.salon.com/2011/10/20/china_says_internet_censorship_meets_global_norms/

[14] http://futurechallenges.org/local/the-internet-freedom-fallacy-and-the-arab-digital-activism/

access citizens' private digital communications than it is for authorities to search or carry out surveillance of our physical homes, offices, vehicles, and mail. Standards of oversight, due process, and accountability have been eroded in ways that have made it easier for government agencies to abuse power and more difficult for citizens to hold the abusers accountable. Close relationships between government agencies and U.S. corporations have cultivated and even encouraged an industry-wide corporate culture of opacity and secrecy when it comes to companies' relationships with government clients and government agencies seeking access to user information that companies collect.

This situation in the United States obviously does not have the same kind of deadly consequences in a multi-party democracy with an independent judiciary, freedom of the press and separation of government powers. I am not trying to equate the situation in the United States with the situation in authoritarian countries – that would be nothing short of ludicrous. Nonetheless, the current environment of secrecy, opacity, and inadequate mechanisms for public accountability in the relationship between technology companies and government here at home is not only corrosive to American civil liberties but also feeds and encourages a broader global culture of secrecy in public-private relationships involving censorship and surveillance.

The U.S. government's working relationship with companies that manufacture surveillance technology is predominantly as an enthusiastic client rather than as a regulator. 35 U.S. government agencies attended the annual Intelligence Support Systems (ISS) World Americas, an annual trade show for makers of surveillance technology, held recently in Bethesda, MD, along with representatives of 43 countries. The gathering was closed to journalists and the public but according to attendees, there is no evidence that these U.S. agencies are making any attempt to use their power as a customer to insist on human rights standards or guidelines in the development, sale, or deployment of these technologies.[15]

Freedom of Information requests by researchers and activists reveal a shocking lack of accountability in government access to corporate-held data. In early 2011, Christopher Soghoian, an antisurveillance activist and doctoral candidate at Indiana University, published a research paper in which he concluded that "law enforcement agencies now make tens (if not hundreds) of thousands of requests per year for subscriber records, stored communications and location data." He also found that the Department of Justice underreports the volume of requests it makes to companies by "several orders of magnitude." Meanwhile, only a handful of companies have even admitted to the scale of requests they receive.[16]

---

[15] http://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO_print.html and http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques-surveillance Also see http://projects.wsj.com/surveillance-catalog/ and http://wikileaks.org/the-spyfiles.html

[16] Christopher Soghoian, "The Law Enforcement Surveillance Reporting Gap," April 10, 2011, http://ssrn.com/abstract=1806628

In January 2011, the Electronic Frontier Foundation (EFF) published a report concluding that, based on its analysis of FBI documents related to investigations from 2001 to 2008, "intelligence investigations have compromised the civil liberties of American citizens far more frequently, and to a greater extent, than was previously assumed." The EFF estimated that based on analysis of documents it obtained through Freedom of Information Act requests, as many as 40,000 violations of law may have occurred during that period. Judicial and congressional oversight of FBI intelligence investigations was found to be "ineffectual." Furthermore, the EFF found that in nearly half of cases in which the FBI abused the use of National Security Letters requesting information, phone companies, Internet service providers, financial institutions, and credit agencies "contributed in some way to the FBI's unauthorized receipt of personal information."[17]

There are many dozen bills related to Internet and wireless technology now in Congress, with several competing ones on cyber-security alone. Most of them aim to address the relationship between American citizens, U.S. companies, and the U.S. Government, or to enhance the security of the homeland and may seem appropriate in the context of American constitutional protections, free press, and judicial independence. But in this globally networked world, even solutions intended to solve domestic problems related to the Internet and wireless technologies inevitably affect the balance of digital freedom and control everywhere on the planet.

One example is the Cyber Intelligence Sharing and Protection Act of 2011, which exempts companies from liability for sharing data with the government, is just one example of well-intentioned legislation that civil liberties groups are concerned will lead to further erosion of consumer privacy as information can be shared without court order or other protections.[18] Governments around the world frequently point to such legislative trends as proof that their own relationships with technology companies are merely in keeping with global norms.

Chinese Internet users who have broken through their own country's censorship mechanisms, including the filtering system popularly known as the Great Firewall, have been horrified to learn about the Stop Online Piracy Act. They are shocked to see U.S. legislation proposing a nation-wide Internet filtering system, and legal liabilities for Internet companies that will compel website owners to proactively monitor and censor users.[19] While the bill is only meant to address copyright infringement, the technical and legal mechanisms are almost identical to those deployed by the Chinese government to control a much broader range of what they define as "infringement."[20]

---

[17] http://www.eff.org/pages/patterns-misconduct-fbi-intelligence-violations

[18] http://www.washingtonpost.com/world/national-security/cybersecurity-bill-promotes-exchange-of-data-white-house-civil-liberty-groups-fear-measure-could-harm-privacy-rights/2011/11/30/gIQAD3EPEO_story.html and http://www.aclu.org/technology-and-liberty/aclu-opposition-hr-3523-cyber-intelligence-sharing-and-protection-act-2011

[19] http://advocacy.globalvoicesonline.org/2011/12/03/for-chinese-netizens-sopa-is-another-great-firewall/

[20] https://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html

Most recently the government of the world's biggest democracy, India, has jumped on the censorship and surveillance bandwagon. According to media reports, India's telecommunications minister, Kapil Sibal, has demanded that companies including Facebook and Google to pre-screen their users' activities to ensure that no derogatory content related to Prime Minister Manmohan Singh, Congress party leader Sonia Gandhi or major religious figures was posted.[21]

In June 2011, UN Special Rapporteur on Freedom of Expression Frank La Rue delivered a report to the UN Human Rights Council that not only condemned the censorship and surveillance practices of authoritarian countries, but also warned of dangerous trends in the democratic world that threaten citizen rights in the Internet age. "Holding intermediaries liable for the content disseminated or created by their users severely undermines the enjoyment of the right to freedom of opinion and expression," he wrote. "It leads to self-protective and overbroad private censorship, often without transparency and the due process of the law." La Rue stressed the need to preserve citizens' right to online anonymity as a prerequisite for dissent and whistle-blowing, calling on governments to refrain from requiring "real name" registration on social networks, as in South Korea. He was also "deeply concerned" and "alarmed" by French and British "three strikes" laws. Cutting off Internet access as a response to copyright infringement, he wrote, is "disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights."[22]

It is clear that the Internet has brought new opportunities as well as new threats to governments, businesses, and citizens everywhere in the world. The United States and other democracies can and must do a better job of demonstrating that economic success and national security will benefit in the long term when they are pursued - in the digital realm as well as the physical realm - in a manner that is compatible the respect and protection of civil liberties and human rights.

To accomplish this I recommend that Congress:

Improve and update export control laws. Existing export control laws require updating in order to remain consistent with their intent in the Internet age, in two ways:

Make collaboration with repression more difficult: Recognizing that no connectivity at all is even worse than censored connectivity, and also recognizing that many information communications technologies have "dual use" capabilities that are used for legitimate security and law enforcement as well as repression, it should nonetheless be made much more difficult for U.S. companies to provide censorship and surveillance capabilities, particularly to countries whose governments have a clear track record of using those technologies to suppress peaceful political dissent. The other panelists at today's hearing

[21] http://www.businessweek.com/ap/financialnews/D9RERAS80.htm and http://india.blogs.nytimes.com/2011/12/05/india-asks-google-facebook-others-to-screen-user-content/

[22] http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

have made a number of excellent suggestions to this end. In addition, the Electronic Frontier Foundation's "Know Your Customer" framework emphasizing human rights due diligence provides a two-point solution:

1. Companies selling surveillance technologies to governments need to affirmatively investigate and "know your customer" before and during a sale. We suggest something for human rights similar to what most of these companies are already required to do under the Foreign Corrupt Practices Act and the export regulations for other purposes, and
2. Companies need to refrain from participating in transactions where their "know your customer" investigations reveal either objective evidence or credible concerns that the technologies provided by the company will be used to facilitate human rights violations.[23]

Require transparency in what is sold to whom and where it is being used: The trade in some surveillance technologies - particularly those that include intercept capabilities - is already restricted: before they can be sent abroad, the Commerce and Treasury departments must approve the export of these technologies. However, the data that these agencies have, detailing which companies have sold what surveillance equipment to which foreign governments is not public. U.S. government agencies should be required to publish such data, so that it can be analyzed by academics, activists, and the press.

Additionally, companies that have data on where their technology is used should be required to publish it. The *Wall Street Journal* recently reported that surveillance devices manufactured by the U.S. firm Blue Coat regularly transmit automatic status messages – which include the serial numbers of each device – back to the company. Company representatives have acknowledged that Blue Coat does not pro-actively monitor these "heartbeat" messages to learn where its filtering technology is in use. Bluecoat did not acknowledge that technology was used in Syria until a journalist presented the evidence to them.[24] They and other companies selling similar technologies should be required by law to report on where their technology is being used.

Halt denial of service to human rights activists: The United States has several laws that bar the sale of specific kinds of software to, or forbid business transactions with, individuals and groups from specified countries. These laws do not take into account new Internet developments, and as a consequence have resulted in denial of website hosting and other services to dissident groups from repressive nations. U.S. laws – exacerbated by corporate lawyers' over-cautious interpretation of them – have in recent years prevented U.S. web-hosting companies from providing services to opposition groups based in Iran, Syria and Zimbabwe.[25] While the Treasury Department's Office of Foreign

---

[23] https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment

[24] http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

[25] "Not Smart Enough: How America's "Smart" Sanctions Harm the World's Digital Activists," by Mary Joyce, Andreas Jungherr and Daniel Schultz, DigiActive Policy Memo for the Commission on Security and Cooperation in Europe, October 22, 2009, at: http://www.digiactive.org/2009/10/22/digiactive-policy-memo-to-the-us-helsinki-commission/

Assets Control is to be applauded for taking an important first step last year in issuing a general license for the export of free personal Internet services and software to Internet users in Iran, Cuba, and Sudan, and an additional step this year to include Syria.[26] However this piecemeal approach is inadequate and needs to be replaced with a general license that clearly allows the export of communications technologies of the kind used by individual citizens to communicate, organize, and express themselves.

Require corporate accountability and transparency in all markets. Companies should be required to report regularly and publicly on how content is deleted or blocked and how user activities are monitored. In the summer of 2010, motivated by its commitments as a GNI member, Google took a step in this direction by launching a website called the Transparency Report, tracking the numbers of requests it receives from governments to take down content or hand over user information, broken down by country. Its latest bi-annual report released in November provides more granular data, including the number of requests that the company complied with or refused.[27] All companies should be required by law to publicly and clearly report on how they gather and retain user information, and how they share that information both with government and other companies. In doing so they can credibly demonstrate that they recognize and take seriously the power they hold over Internet users worldwide in our relationships with our governments, and they understand their duty to wield that power accountably so that people are fully aware of the risks they face and know who to hold accountable for abuses.

Mandating greater accountability and transparency on the part of corporations as well as government about how citizens' communications are censored or monitored can help to stimulate what security researcher Christopher Soghoian calls "a market for effective corporate resistance to government access." Soghoian points out that when most people choose their broadband provider, mobile phone service, web-hosting service, social networking service, or personal e-mail provider, company policies and practices in dealing with government surveillance are rarely considered. Part of the reason is that it is very difficult for an ordinary person to know what each company is doing and to compare company practices in a meaningful way. Congress can help to change this situation.[28]

It is also essential that shareholders and investors have access to adequate information about what they are supporting – whether or not the business in question is technically complying with current law – so that they can make informed investment decisions based not only on financials but also on the kind of world they desire for themselves and their children.

---

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

[27] https://www.google.com/transparencyreport/

[28] Christopher Soghoian, "An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government" (August 10, 2010), *Minnesota Journal of Law, Science & Technology*, at http://ssrn.com/abstract=1656494

Support multi-stakeholder corporate accountability efforts like the Global Network Initiative. It is clear, given the rapid technological and geopolitical changes over the five years since the Global Online Freedom Act was first introduced that legislation and government action – while essential – are likely to remain inadequate on their own to address problems faced and sometimes created at the same pace that technology businesses are launched, evolve, and innovate. While law can and should mandate over-arching requirements, independent, rigorous, and accountable processes for evaluation and assurance of corporate practices, conducted in a manner that address constantly-evolving challenges of global technology businesses, are essential if corporate reporting is to be meaningful or credible. Requiring human rights assessments and reporting is not enough if corporate claims are not independently and credibly verified. Thus active and direct civil society and investor participation through multi-stakeholder initiatives such as the Global Network Initiative is and will continue to be critical in holding companies accountable.

The Global Network Initiative's globally-applicable principles on free expression and privacy are supported by implementation guidelines and an accountability framework that applies to all markets and can be adapted to a range of business models, including hardware companies and Internet service providers. All companies in the information and communication technology sector should be required not only to recognize their human rights risks and responsibilities, and conduct human rights due diligence, but also to submit to an assurance process that is at least as independent and rigorous as the GNI assurance process. Companies that choose not to engage with the GNI should be required to submit to a multi-stakeholder-driven assurance process of proven rigor and independence.

Ensure that all U.S. legislation is compatible with global Internet freedom. Before being introduced, all bills involving Internet regulation should undergo their own process of human rights assessment and due diligence. They should be thoroughly reviewed by staff specializing in human rights and global Internet freedom issues, in consultation with independent academic experts, to identify potential impact on human rights, free expression, and global Internet freedom.

Thank you once again, Chairman Smith and Ranking Member Payne, for the opportunity to testify before your committee today. You are to be commended for your persistence and concern for global Internet freedom at a time of economic uncertainty here at home and contentious debates about our nation's future course. As today's discussion has shown, there is no one-shot "silver bullet" for achieving global, long-term and sustainable Internet freedom. Offline physical freedom here in the United States - or anywhere else for that matter - was not won easily, and will not be expanded, preserved or protected without constant struggle and vigilance. Internet freedom is no different. A global struggle for freedom and control of the Internet is now underway. As with our physical freedom, Internet freedom will not be possible without an ecosystem of industry, government, and concerned citizens working together with a shared commitment to basic human rights and values.

Mr. SMITH. Let me ask, maybe start off with you and the others who might want to speak to this, China, it would appear, and I just chaired a hearing a couple days ago on Liu Xiaobo. A year ago on Saturday, we had the sad and tragic situation of an empty chair in Oslo where neither he, nor his wife, nor was anyone else able to receive the Nobel Peace Prize that he so richly earned by his advocacy for democracy in China. We know that the Chinese Government has deployed huge resources, no one knows the exact amount, but we know the consequence, to surveil and to use every means of making as impenetrable as possible the Chinese Great Firewall, and I know that a number of very talented people, including some from the Falun Gong and other very talented people who have been able to breach it have come up with technologies that are very useful not just for China, but elsewhere.

A couple questions. Has China turned the corner with its own indigenous corporations, like Baidu and others? You know, they were totally relying or very much relying on U.S. high tech companies like Google, Microsoft, Cisco, and Yahoo! early on, but have they now taken the baton and created their own capabilities that parallel or even exceed those big corporate giants? And do you believe that if we require a listing of their due diligence efforts as being part of the U.S. stock exchange, which the new Global Online Freedom Act would require, would that be a helpful tool in knowing what, for example, Baidu is actually doing from year to year?

Ms. MACKINNON. Thank you for those questions. In China today, actually, a great deal of the censorship and surveillance is not actually being conducted by the government. It is being conducted by Chinese companies largely. Most Chinese Internet users today, when it comes to social networking sites, when it comes to search engines, are primarily using Chinese services, and while Western hardware providers are certainly doing a great deal of business in China, Chinese companies such as Huawei, which is often called the Chinese Cisco, and another company called ZTE are also increasingly competing with Western products and are also innovating in terms of standards in a range of ways, and so, yes, China definitely no longer relies on Western technology to run its Internet infrastructure or, I should say, no longer needs to rely on it, and certainly when it comes to the Web, the Web tools, social networking, and search engines, again, that market is almost entirely domestic, and all of those companies are required to monitor and censor users, and they are doing it not with Internet police coming into their offices, but they are employing their own employees to conduct this censorship and monitoring, so the private sector is actually subsidizing a lot of this control.

Speaking to your second question about reporting, I think this is quite important for a number of reasons. The first reason is that I think a lot of American investors who are investing in these companies do not really understand what is happening and do not have full information about the relationship between the government and the private sector and the Internet companies in China, and so requiring reporting in that regard would enable investors to make more informed decisions about what they really want to be supporting.

Furthermore, reporting requirements would help Chinese people understand what is happening because, of course, most Chinese Internet users actually don't realize the extent to which these companies are censoring and manipulating and monitoring them because they are living within the system itself. They have been living with blinkers all their lives, they are not aware of what it is like not to have blinkers. So most definitely, greater knowledge, greater public awareness of what companies are doing will help inform users of what the alternatives are and what other possibilities might be.

Mr. CALINGAERT. If I might add, I think there is a serious question of whether the Chinese companies that Rebecca mentioned are benefiting from protectionism. There are indications that the major American social media companies like Facebook are often blocked in China, and that probably benefits the Chinese companies commercially. There is a recent case reported of an application for iPad called Flipboard which aggregates news, and they launched recently in China and were blocked because they were providing the kind of content that the Chinese Government objects to, and there just happens to be a Chinese clone for this kind of application, and, you know, the reports are still being fleshed out, but there are indications that the American company was told that the Flipboard application, unless they started censoring, they would essentially lose out that market share to a Chinese company. So I think this, and especially the trade provisions of the GOFA bill, will get at this kind of problem.

Ms. MASSIMINO. I just want to echo that and say that I think that the SEC reporting provision in the bill, it is one of the most important provisions. I think that this is incredibly important for all the reasons that you heard, especially, I think, for transparency for investors. This is going to be a key issue. I think that as much as the industry has developed in China, the Chinese market is always going to be a huge magnet. You combine that with the fact that this is a business that is all about innovation. I think that it is going to be, in an ongoing way, very, very important to make sure that we are advising and requiring American companies or anybody, any company that is listed in the American stock exchanges to make these disclosures.

Ms. LE COZ. I also would like to add that asking Baidu and other companies about what they are doing is also very timely. It is not only necessary, it is now because last month, the Chinese Government convened a meeting of the top 40 Chinese companies, Internet companies and high tech companies, to adopt new guidelines, so if there is a time where you can ask what they actually are doing is now.

Mr. SMITH. I appreciate that. Again, that is one of the improvements to the bill that we did not have in the existing or the preexisting proposals. On the export controls issue, if you would briefly touch on that, you know, it seems to me that even though a parallel industry has emerged in China, aided and abetted by U.S. and other high tech companies in the West, obviously the next advancement, the next capability, is always right around the corner, and if people do find the means to pierce the Chinese Great Firewall, if we are providing surveillance and censoring capabilities that are

the next generation, it seems to me that it would be in our humanitarian interest not to be exporting it. Would you agree with that? Is that an important component here?

Because, obviously, they are still buying the next-generation technology, software, hardware, from U.S. corporations, and just as we wouldn't sell to their police certain police equipment, I hope we wouldn't sell them implements that could be used in torture, while certainly this is an area that is being used grossly for repression.

Ms. MASSIMINO. Yes, I can just start. But I think that is incredibly important. This is Section 301 in the bill, it is very important, and it is incredibly timely. There is an obvious gap, we talked about it today, that companies are able to say what we are doing is not illegal. We need to change that.

I think another reason why that provision is important is because so many of these companies really have not gotten their heads around what it means to be responsible for the end use of their products. And a provision like this will force companies to ask those questions and to understand what it means to do due diligence. In many of these companies what we have found is they have just not yet realized the extent of their obligation. And this is, I think, a very important way to do that. We have asked these questions of companies, many of the companies that you heard us talk about today, whose products have ended up in the hands of repressive governments and about what they did to protect against that. And the answers, I can share them with you and your staff, are very revealing. Some of them had no idea that they even had to think about this. Others thought that a private company in the United States, private business partner that you are selling to, is the same as a private company in Iran, and others think that they have no obligation at all to disclose what they do or who they do it with.

So I think this provision will go a long way to underscore with companies the extent of their only obligation, and it will prompt better due diligence in the future.

Mr. SMITH. Before the others answer, your excuse number four, that somehow this is a force for good, hopefully that myth—and I think for some, it was a well meaning sense. Google told us that when they testified here they thought the Internet would be opened up. As you mentioned earlier, Ms. McKinnon, in your quote that somehow there is something inevitable about the Internet that will open up societies. No, not when it is in the hands of a dictatorship. So I thought the force for good argument, hopefully that could be laid aside a couple of years ago, and certainly today, because it is being used maliciously.

Ms. MASSIMINO. Absolutely. And you know we hear from companies all the time that the real bad guys in this equation are the governments. And of course, that is true. But governments need tools in order to do the bad things that they do, particularly now. And for companies to ignore the potential for complicity in that chain of events I think is irresponsible. And this bill will help companies understand their responsibility in that chain.

Mr. CALINGAERT. I would like to add a couple points. I think the approach that GOFA takes makes a lot of sense for a field or an industry that is very rapidly changing and you probably know all

too well from having to update GOFA now for the third time, that changes in technology have a big implication for how you write the law.

By focusing on basically setting in place a system to control exports, defining the kinds of export that you want to prohibit, what exactly is damaging about the technology, identifying the countries that should be on the list, and then presumably the list of actual technologies and products can be updated as you go ahead.

I also think it is important that with this bill, you try to get ahead of the next scandal that is going to happen. I mean, sadly, there were the reports of Cisco helping build the Great Firewall of China and then afterwards policy makers trying to figure out how to fix that problem. And then you had the Yahoo! case, and you had Nokia Siemens selling surveillance technology to Iran. And there is nothing out there to stop yet another company doing who knows what. And so I think it is well beyond time to get ahead of this problem and put in place the system that is going to prevent the next abuse.

Ms. LE COZ. Reporters Without Borders was really pleased to see that new provision, and we would like, actually, to encourage you to reach out to the European Union once they implement the European GOFA. That would be a way of being effective worldwide. And not to not sanction any U.S. companies who would like to do business abroad but who has to compete with the European one who wouldn't have to face the same challenges.

And still regarding that provision, what we would also welcome is a way of asking companies to track down their technologies because they might sell it to a country that is not specifically repressive or not on the list, but it might still be able to go there. So to actually have a means of knowing where the technology is.

Ms. MACKINNON. Just to add on, I concur with pretty much everything everyone said, but just to add a couple of points on both the "it is not our responsibility to know how the product is used" type of excuse, "because we are not doing anything illegal," and also the excuse that, "well, we are a transformative freedom-bringing technology anyway, and so those little details don't matter so much because in the end everybody is going to be freed by the Internet anyway," is sort of the narrative you often get.

And what is quite funny is that this particular industry, while claiming to be so much more advanced than anyone else, any other industry, is actually a laggard compared to the extractive industry. Oil and gas and mining companies have long ago recognized that they cannot go it alone, that they need to be held accountable to work with other stakeholders, to work with human rights groups, to work with socially responsible investors to figure out how to mitigate their human rights risk. That industry, for the most part, they are not perfect—but at least a lot of these companies have come to recognize that they do indeed have human rights risks, that they need to acknowledge them and they need be to held accountable to their commitments, and they need help reaching their commitments.

Similarly, in the manufacturing and apparel industries on labor standards, you also have companies recognizing, the old tech companies, recognizing that they have human rights risks and respon-

sibilities that they need to work on and accepting that they should be held accountable.

Yet for some reason the technology industry seems to have an attitude, with only a very few exceptions, this kind of holier than thou, we are so Messianic, that we are above having to be held accountable or having to admit there is any downside to what we are doing. And it is time for people to grow up.

Mr. SMITH. Well put.

Mr. Payne.

Mr. PAYNE. Thank you very much. Let me thank all of you for your testimony, and I couldn't agree with you more.

Some of these companies talk about the difficulty that it is to monitor and so forth.

We had the same kind of notions that were expressed when two different types of legislation came about as related to Africa, the first being the blood diamonds legislation. People said there was no way, you can't identify diamonds, and as you may recall, in Sierra Leone, the diamonds were used by Charles Taylor to fuel the civil war and so forth. But we were able to get the Kimberley Process. It was strained. There was opposition to it. There were people who said it couldn't be done, but it is happening. It has got to improve, but it is happening.

We have a second legislation that is working its way through, the minerals bill, I forget the exact name, but it is going to do the same thing in the Democratic Republic of Congo and other areas where minerals, very valuable minerals, are being used to fuel wars and that warlords are taking the profits, not benefiting the standard of living for the people in that country, very rich but one of the poorest for standard of living in the world, and we are moving that process through.

So what do these Internet companies say? Is it impossible? Or is it that they just simply don't want to take on that socially responsible position?

Ms. MASSIMINO. Well, I think, they say a number of things, and I try to outline them in my testimony. These are the excuses for why they can't be held accountable or they can't know, and while I am sympathetic to the argument that companies can't control everything, it doesn't follow from that that they can't control anything.

And I think that is one of the things that we are struggling with, with some of these companies.

Now, of course, there are going to be lots of factors outside of companies' control and outside of the U.S. Government's control, frankly. But that doesn't mean that we can't significantly improve the performance and improve the situation for people in these countries who are struggling to advance freedom of expression and human rights in their own societies.

Companies have to feel that they are being watched, their performance is going to be evaluated and that, particularly American companies, that we, as a country, stand for something and a lot of what we are exporting to the world is the values of our private industry. And those are important.

When we are able to do this, it can work. If you remember the example of, and this gets us to the intellectual property issue that

you heard about before, when companies are made to understand their role in repression and/or work with civil society and governments to fix it, it can be fixed. Remember what happened with Microsoft in Russia, where the intellectual property in piracy enforcement action against pirated software was being used by the Russian Government to crack down on dissenters or a civil society that was critical of the government. And Microsoft was complicit with that because it was frankly just dealing with the law enforcement entities in Russia the way they would with the law enforcement entities in the United States, rather naïvely, I think, under the best interpretation of their actions. But when made aware of that, and when they realized that they were complicit in the crackdown on dissent by the Russian Government, they changed. And they put their know-how and their innovation and their good thinking that they put into the development of their products into fixing this problem and came up with a scheme working with and speaking with civil society in Russia and here to circumvent the Russian Government's misuse of intellectual property enforcement and gave a blanket license to these groups to use their software.

So it can be done, but requires a lot of vigilance on the part of the U.S. Government and civil society and working together, as Rebecca said, in these multi-stakeholder initiatives to be able to surface these issues.

Mr. PAYNE. Thank you very much.

Ms. Le Coz you mentioned in your six or seven points at the end of your testimony that we should encourage other companies, especially members of the OECD, to adopt similar bills.

How has the effort been, and any of you might want to participate in the answer if you have something to add, how has the effort been? What has been the response from the European, the OECD companies? We hear, as you know, American companies say, we are at a disadvantage; we have the laws that, for example, business laws that prohibit corruption, the Foreign Corrupt Practices Act, for U.S. businesses that makes it illegal to bribe countries and contracting and so forth.

European countries still have that provision. It is not illegal, and up until recently, it was actually a tax deductible item in Germany; it was just considered, just reported, as a cost of doing business. But I wonder how are the Europeans dealing with this, and has it come up? Has there been a concerted effort? Has any country taken this issue on?

Ms. LE COZ. Yes. The European Union would like to implement GOFA in Europe, but they are not as far as the United States are. From when I just came to the Internet freedom desk for Reporters Without Borders, we were a part of the negotiations for what became the Global Network Initiative. You had European companies that were in those negotiations. They ended up never signing it, and when you were asking them why—and please, jump in as we talk about it—but when we were asking them why, it was, they didn't expect it to be that important.

It means that at the level of their own companies, they had to hire and create something on human rights and business practices, which, and in that sense, where you were saying that, would the American companies say it is possible or impossible? I would say

that the American companies, they are a lot more than what the Europeans have been so far.

There might also be a difference in the way they see it. You try to prevent, and maybe in the European Union, we had the sense that it had happen to react.

Mr. CALINGAERT. If I could add, the Foreign Minister of the Netherlands has called for export controls, and also there was a vote in the European Parliament in April to introduce export controls on technology to monitor Internet use and mobile phone use. In the European system, obviously, that kind of initiative won't happen until the European Council approves. But I think there is significant movement in a similar direction to GOFA.

And I would also note that much of the interest, I know from discussions with Dutch, Swedish and other European officials, they are very interested in this issue in large part because of the Nokia Siemens case. It was really a disgrace that two major European companies sold very sophisticated monitoring technology to Iran which was used to clamp down on dissidents after the 2009 election.

And these most recent reports of technology going to Syria and what was sold to Libya under Ghadafi originated in Europe as well. So I think this is a very salient issue. And there is a real opportunity to coordinate with European policymakers so that if and, hopefully, when export controls are introduced in the U.S., there are similar controls introduced in Europe and neither side's businesses will be disadvantaged.

Mr. PAYNE. Thank you. Let me just ask one more question.

As I indicated in Africa, we know about the Mugabe government and what is happening in Ethiopia, and I just wondered to what extent are African governments attempting to monitor or control private digital expression, in particular to exert political control over communications and how can citizens more effectively counter state attempts to control digital communications in these countries?

I don't know if any of you have focused in on Africa other than the two countries that we cited. Yes.

Ms. MACKINNON. Just a few comments. Ethiopia definitely filters the Internet. I think Zimbabwe less so, but it is believed that there is a certain amount of monitoring going on and other panelists may have other information.

But it is also true that a lot of countries in sub-Saharan Africa are heavy customers of Chinese networking equipment, Huawei and ZTE in particular. And it is difficult to get a lot of details about the types of customization that goes on and so on. But just given how the network is configured in China and given some of the regimes that this equipment is sold to, we can easily draw some conclusions.

Mr. PAYNE. Thank you.

Yes.

Mr. CALINGAERT. I just add briefly that the "Freedom on the Net" report of Freedom House covered several African countries, and Ethiopia was rated "not free," among the worst rated countries; Zimbabwe, "partly free." And the reports themselves have a lot more detail that could answer your question.

Mr. PAYNE. Thank you.

Well, I think that we really need to start to come down and push these technology companies, as you mentioned, to grow up and to have a human rights component as a very important part. There was a debate back 6, 7 years ago about whether restricting the Internet was going to harm or help the emergent countries. And at that time, being a former educator I felt that well, the ability to have information unrestricted, or information in general, if some is restricted, perhaps the overall good outweighs; that is what the arguments were at that time. And I was watching it from that point so-called balanced approach type thing.

Certainly, it appears as if these corporations really are putting human rights and other issues far behind. It is just about doing business, about doing more business, and if some people are harmed, well, then, that is I guess maybe the cost of doing business.

And so I do think that we need to start looking at stronger restrictions, and hopefully, it would be great if all these companies would just say, we are going to do the right thing, and then if a company wanted to do use any Internet, they would have to comply to what all these companies say. It could be a reverse way, where they say, well, none of us will go into, say, China or go into Zimbabwe, period, close them right out, and the country can't be left without it, so then if that sparked the countries to say, well, maybe we need to relook at ours; we can't be shut out; we can't be left out of this new millennium, perhaps something like that, of course it is a great dream, but something like that could put pressure on a country to say, I guess we need to change or we are going to be left behind big-time.

So maybe that notion could kind of be thrown out there at some point.

Thank you all very much for your testimony.

Mr. SMITH. Thank you Mr. Payne.

Let me just ask a few final questions and then if Mr. Payne has any additional.

Ms. MacKinnon, as a board member of the Global Network Initiative, you certainly have a ringside seat as to how well or poorly voluntary corporate responsibility is playing out, and I would note parenthetically, on the day we held the hearing, the first hearing ever on global Internet freedom, which led to the introduction of GOFA, the State Department came and sat where you sat, and announced the task force, the Global Internet Freedom Task Force, which to some extent took the wind out of the sails of one of the first provisions of the bill which was to create an office at the State Department. A task force is not an office, but it certainly has capabilities, and we welcomed it, I welcomed it, with open arms because it was moving from nothing to something. But very often we see this across the board on human rights issues, we are always told, let the companies comply voluntarily—and some do you; there is no doubt about that, some do step up to the plate.

I remember during the early years of my tenure in office in the 1980s, I got elected in 1980 and took office in 1981, the same argument was being employed to say, "Let's not have sanctions on South Africa," such arguments were being used on a whole host of

human rights issues with regards to Eastern Europe, and it never worked, until you said, "We are not kidding." We even have some companies argue that there is a competitive disadvantage to doing due diligence on human rights when the competitor is not, so they don't want to go that route, so the corporate board sits around and says, "Let's eschew that."

So if you could speak to the Global Network Initiative, the GNI, because it seems it has had time to prove itself. The State Department finally, I don't think has stepped up to the plate and said—and the Pentagon—that there are real security implications that are underappreciated about what is happening here, all this police capability that has been significantly enhanced also has dual use for militaries that are deployed elsewhere I would think. So if you could take a stab at that.

Ms. MACKINNON. Well, thanks very much. And just to emphasize, I do agree that government pressure, Congressional pressure and pressure from the executive is extremely important. And without that pressure, it is difficult to properly incentivize, let's say, companies to move in the right direction. And GNI is certainly meant to be part of an ecosystem of efforts, it is not meant to be the end all or be all by any means.

I think as far as the success of the initiative, it is still in the early days. Those who have been involved with some of the other multi-stakeholder initiatives around extractives, blood diamonds and manufacturing, will know that it takes sometimes a few years for these initiatives to really prove themselves, to gain membership and so on.

And the first round of assessments is currently underway. The assessments, the independent assessments of the first three companies to join, Google, Yahoo! and Microsoft, will be completed early next year, and the results will then be publicized. We will have a better sense by then of to what extent membership in the Global Network Initiative has in fact improved these companies' ability to address their responsibilities and to avoid problems.

But it is definitely true there is a problem convincing companies that they need to do this. And with a small staff and a small membership, GNI cannot on its own convince companies that they need to be held accountable and that they need to make commitments. If consumers are not aware of what is going on, if investors more largely are not aware of what is going on and if there is insufficient government pressure, if there is no kind of disincentive from other parts of the government, then there is going to be a lot less reason that they are going to feel like they should expend the effort.

I would also point out, too, that, and again, I agree that well-crafted legislation is an essential part of the picture, but there are also aspects because technology evolves so fast, it is difficult to get too finely grained about each specific company because every company, every technology is somewhat different. Their technologies are changing very quickly. In 2006, when GOFA was first introduced we were mainly talking about filtering, now we are talking about deletion and deep packet inspections and surveillance, and the technology has evolved a great deal, and so it is difficult to revise and refine and change the legislation in a very finely grained way so that companies don't then come up with this excuse, well,

it wasn't illegal, so we did it, because you didn't get around to passing the law or changing the law.

And so one of the benefits of having companies make broad commitments to free expression and privacy and then work with—in a sufficiently robust multi-stakeholder initiative that holds them to these commitments is that you can then have a group of experts really looking at the very specifics of their technology and the very specifics of how it is affecting users from month to month and year to year as that changes very rapidly and make sure that they are living up to the spirit rather than just the letter.

And keeping companies connected with the spirit, I think, requires more than just law. It requires an ecosystem of efforts and an assurance and assessment process that is independent and that has the involvement of human rights groups and technical experts I think is also very important.

So it is very early days, GNI now has two new members, and again, we will see how things evolve. There are discussions with some other companies, not only in the United States. We are optimistic that over the coming months, there may be more members.

I think a growing number of companies are recognizing that they do need help and are starting to think internally and have conversations about how they get to the point where their corporate culture is even capable of joining something like GNI, but there are a number of companies who are starting to move in that direction.

Ms. MASSIMINO. Human Rights First also is a founding board member of GNI, but we have also been involved in a number of these other multi-stakeholder initiatives with private companies. And I would encourage you, one of the reasons for the GNI coming into existence was the perfect storm of pressure, from both the Congress and the public about what companies were doing and the human rights impacts of their actions.

My concern now is that some of that pressure is waning, and there is, as we go through the process, as Rebecca said about, you know, implementation of the principles and assessment of companies' performance, that there is a bit of a waning of energy in terms of the urgency of commitment to that.

You know I think for us, the metrics for success for the GNI or any other multi-stakeholder initiative like that is not so much the number of company members, although that is important, we want more companies to join, but we want them to join for the right reasons. And I think it would be very instructive and helpful actually if you and other leaders on these issues in Congress were to keep an eye on the GNI and ask us questions about how we are doing, perhaps even have a briefing or a hearing about, once this initial assessment phase is done. Transparency is so much the key to getting this issue right. That is why the provisions of GOFA that require reporting are so important. It is also the key to these private multi-stakeholder initiatives working.

So I would ask you to encourage us in the GNI to be forthcoming about that and ask us the hard questions.

Mr. SMITH. We will invite you back on that.

Let me ask Ms. MacKinnon, with regards to the export of China's capabilities, specifically by Chinese companies—and I do think when we talk about China's private sector, it needs to be in quotes

because it certainly is heavily influenced if not run by the government—but, are we seeing an exporting of Chinese capabilities to other repressive regimes, like Belarus, like Egypt, for example, or anywhere else?

Ms. MACKINNON. Certainly Chinese networking companies like Huawei and ZTE, who I mentioned, are doing a lot of excellent business in much of the world. Libya was a heavy customer of Huawei's. We are finding out Iran is a strong customer of theirs as well, and so certainly the capabilities of their networking equipment and their willingness to service that equipment in ways that suit those local governments' needs is certainly helping those governments to filter and monitor their networks.

But the problem is that we are finding actually the most sophisticated surveillance technologies that are making their ways in the Middle East and North Africa and also in other places, these are actually coming from the West. And so this is part of the problem, is that the highest tech surveillance mechanisms are really coming from us.

Mr. SMITH. Let me ask and maybe Dr. Calingaert, you might want to answer, one of the provisions in our trafficking in persons law heavily emphasizes naming and shaming, naming countries—and there is obviously a follow up, once they are named; when they are designated a Tier III, for example, they can be very heavily sanctioned. We do the same thing with Countries of Particular Concern for religious persecution issues and religious freedom. And the first provision of our Global Online Freedom Act is Internet restricting countries. I have absolutely no doubt there will be pushback from the administration, as there always is, no matter who is in the White House, that they don't want to make such a call, but it has been my experience, especially with trafficking, that when a country is even on the Watch List but they are a Tier III, I talk to them; Luis CdeBaca, Ambassador-at-Large for trafficking issues, his office is deluged. Our local mission of the named country is visited, a dialogue starts, and very often, that country, through very real, concrete actions can get themselves off of Tier III by taking action to try to combat to human trafficking. Will that work here? Do you think it is a good idea to have such a designation for countries that engage in that?

Mr. CALINGAERT. Absolutely, and in some ways, it might work better because with Freedom House's report, we already do this. And it is an entire report looking specifically at the issues of access, restrictions and other challenges to Internet freedom.

If we are looking at the how it might apply, we use the most simple summary of our results, put countries into three categories, either "free," "partly free" or "not free."

In terms of Internet freedom, our last report covered 37 countries; of those, 11 were rated "not free." And by our assessment, it is very clear that the restrictions on the Internet in those countries are quite extensive.

The bigger challenge is what to do about the mid-range countries. And there are several countries in the partly free category where there are quite significant restrictions on Internet freedom, but the interesting point is there is much more freedom on the Internet than in the traditional media. And, in fact, we use the

same scale for our press freedom as we do for Internet freedom, and it is precisely in this mid-range where we see a big gap showing much more Internet freedom than traditional press freedom.

That said, there are certain countries in that category which we are very concerned about, including Malaysia and Russia, and we are looking closely at the trends there because we think the environment might get a lot more restrictive, and especially Russia, after what has happened in recent days that the Internet was instrumental in exposing a lot of the vote fraud, I wouldn't be surprised if the Russian Government starts to clamp down there.

Mr. SMITH. Ms. Le Coz did mention denial of service in the Russian context as well.

Ms. LE COZ. Yes. Last week, 15 Web sites were attacked in Russia and right during the parliamentary election.

Mr. SMITH. Including the chief monitoring Web site, isn't that correct, for independent assessments of how free and fair the election was?

Ms. LE COZ. Yes.

Mr. SMITH. Let me ask just a few final questions. Corporate responses to enabling repression can take either ignorance—and we had that at the first hearing, I sensed that some whether wittingly or unwittingly, some of the top people, some of the brightest minds in Google, Cisco, Microsoft and Yahoo! kind of were feeding an ignorance that somehow what they were doing, "Gee us?" Some of it might have been real. But there is also the indifference, somebody could just be indifferent; they don't care who gets hurt as long as they make money. But recently the President, Jerry Lucas of the company that hosts the Wiretappers' Ball, a surveillance industry trade show, told the Washington Post that this technology is absolutely vital for civilization. He told the Guardian that an open market exists for the sale of technology and that you cannot stop the flow of surveillance equipment. He suggested that it is impossible to control this equipment.

An anonymous State Department official who attended the Wiretappers' Ball in Maryland told the Washington Post that "we have lost, if the technology people are selling at these conferences gets into the hands of bad people, all we can do is raise the costs; we can't completely protect activists or anyone from this."

Now that sounds to me more like surrender, and if we just throw up our hands and say, no mas, we have lost the ability, I think, to protect the best and the brightest in all of these countries who just want to be free and have a democracy.

What is your sense when you hear that kind of statement from the State Department and Jerry Lucas in his comments?

Ms. MACKINNON. If I may, well, Jerry Lucas is amoral, if not immoral. Those types of statements are certainly unacceptable.

I think, however, it is also important to point out that the U.S. Government's relationship with many of these companies is more as a client and an enthusiastic client than as a regulator or putting any kind of pressure on them. I have heard of no evidence that the several dozen U.S. agencies, State and government agencies, as well as Federal that attended that conference, have made any effort to use their pressure as major clients and customers of these companies to ask questions about whether these companies are ac-

tually adhering to human rights norms, whether these technologies can be modified in ways that go far beyond the way they ought to be used in a free and democratic society.

And they are just going there to buy and find out all the cool things they can do and are basically to some extent complicit in this culture of secrecy and basically anything goes, you just sell this to whoever wants it, and you have got U.S. Government agency people in these meetings rubbing shoulders with people from governments all over the world. And it is basically a secret meeting. The press isn't allowed to come. There are no requirements to report on what goes on there.

And I think it is important that the U.S. Government take the lead in adopting policies of greater transparency and accountability about how these products are being used and the U.S. Government's relationship with some of these companies that we know are complicit in repression around the world.

And if I could add one further comment on the designation, I think that the naming and shaming component definitely can be quite effective or has been shown to be effective in other kinds of human rights situations.

With the Internet, one thing we do need to be careful about is how we use these designations, how we then, the requirements we place around companies and countries that are either designated or perhaps not designated or perhaps borderline so. For instance, one, while there are some countries that might quite obviously fall on the list, there are other countries, such as India, where the Telecommunications Minister has just recently demanded that Facebook and Google and other companies censor political speech on the Internet that they feel is critical of existing politicians. This is an example of why reporting requirements need to be global, that companies need to be transparent about the way and about the extent to which they are handing over information to governments and the extent to which they are being asked to take down content globally.

And I think a good model for this is Google's transparency report where they are reporting on all of the markets where they are doing business, on the number of takedown requests they are receiving from governments, the number of requests for user information they are receiving, and they are also reporting on how many requests they actually responded to and so on. And while, obviously, in genuinely unfree countries, this provides very useful advocacy information for activists, even in countries that might not perhaps make that list, such as India, I know of activist organizations in India who have taken information they have received from the Indian Government about censorship policies and then compared it with Google's transparency report, seeing massive discrepancies and are then able to use this as an advocacy tool to push for greater honesty on the part of their government.

So this is one example, I think, of why it is important that the transparency and accountability reporting requirements and disclosure requirements really do need to be global, because there are a lot of countries where the abusive technology can take a country that is decently democratic and move it into a much more repressive direction. And you want companies to be on the forefront of

helping citizens prevent that from happening in advance rather than waiting until it has already turned into an Internet restricting country and then you place requirements on companies doing business there.

So this is kind of one example, I think, of why global transparency is really important.

And also, I think it is important that democracies take the lead in saying, look, we believe that the relationship between government and companies needs to be transparent and accountable, and that citizens of democracies need to understand what is going on, so that if there are abuses, those can be addressed, and so that we can serve as an example for other countries to follow.

So, again, this is why I feel that a lot of the requirements are best off if they are truly global, even if there is a designation list.

Mr. SMITH. Yes.

Mr. CALINGAERT. I found it really shocking to even get that quote published in the record that essentially some businesses have the attitude of, we just sell this stuff.

We should really pay attention to what this stuff is. When we are talking about spyware, it is software that has gone to some of the worst, most oppressive regimes that we know routinely track, monitor, harass, intimidate dissidents. We know of cases in Bahrain, Iran, and elsewhere where activists have been shown intercepted private communications when they were being interrogated, and they were pressured through that to turn in other activists, and some of these people were tortured. So this is what some Western companies are complicit in.

And sorry, comment on the administration's attitude, yeah, they are throwing up their hands, and that is all the more reason why Congressional leadership is needed on this issue.

Ms. MASSIMINO. Just on that last point about the administration's attitude. My own experience is that that comment from an unnamed official, while it might express some frustration, justifiably so, at what was going on at this conference, doesn't really reflect the attitudes of the people that I have seen working on these issues. I think if there is one thing we know about this industry it is that it is constantly innovating, and so what that means in the context of repressive government and democracy human rights activists is that this is a cat and mouse game, constantly changing. And we have a side in that fight, you know, the United States stands for something, and we are choosing sides, and American companies need to be put to that choice as well.

But as soon as that technology gets in the hands of repressive governments, we also have an obligation and companies ought to put all of their energies and innovation into creating a market to get around that threat to privacy and free expression. And so whatever we can do and whatever the Congress can do to encourage that kind of innovation and transparency about business relationships, that will make sure that the balance doesn't get tipped permanently to the side of the repressive governments.

Ms. LE COZ. I want to add also, we were shocked to hear that comment, and because we sell stuff, 2 years ago, because people sold stuff, there is an American citizen, who is originally from Thailand, who was interrogated on the U.S. soil by Thai officials

simply because of what he wrote online. It happened here. So if you continue to sell stuff, this is actually what people are exposed to and not only in China or where actually these companies want to do business but don't really want to know what the dissidents are becoming once the technology is there, it can come here. It already did.

Mr. SMITH. Before yielding to Mr. Payne, I have always argued that for a dictatorship to prosper and to continue to repress its own people, it needs at least two major components: A very aggressive secret police that can use billy clubs and whatever, to repress its people; and propaganda. It seems to me that in a very real way this high tech complicity, again wittingly or unwittingly, I think, at this point, I don't know, just defies credulity.

We have a situation where, just like tasers are subjected to export controls, this is a taser of high tech capability, and the people who then get caught in its net, and that would be the dissidents, the religious believers, the workers' rights advocates, who, in China, as we all know, are rounded up—there are no independent trade unions and yet if you try to form one or initiate a wildcat strike or, say, you want to negotiate in a collective bargaining, means forget it, you are going to prison. And if you are on the Internet, they are going to find you. So I just do think that tasering is an apt description because at the end of the day, it is the people that we care so much for, the democracy activists, the people who believe in freedom, who are getting tasered by these by the secret police courtesy of high tech companies here and abroad.

So we are going to push very hard.

I do believe, and maybe I'm wrong, but every single human rights initiative that I have been a part of, including the Trafficking in Persons initiative, the TVPA, Trafficking Victims Protection Act, was strongly opposed by the administration. In most cases, they came around at the end and actually signed the bill, whoever it was in office, in that case Bill Clinton. Their folks testified here that they didn't want it. They wanted a couple of small tweakings but not the naming and shaming, not the TIP report, all of those important aspects as well, so I suspect we are going to have an uphill battle here. But frankly, the stakes are so high now, not just for China but for all of the other countries that now have learned from China to use these repressive tools. It is a high tech example of what was said infamously during the Soviet years, the West will hang itself, and they will sell us the rope, and high tech rope is certainly all of what you have so brilliantly testified to today.

Mr. Payne.

Mr. PAYNE. I wonder, I heard you talk about what has happened after the results of the Russian elections have come out. Does anyone have any idea whether the Internet played a significant role in the surprise that Putin had at the results where he did not, I don't think, win an overwhelming majority—I think it was almost less than 50 percent—but do we have any intelligence to know whether the Internet was active there?

Ms. MACKINNON. I can speak to that. Global Voices Online, the Web site that I cofounded, has a team of Russian bloggers and Russian speakers who have been following the Internet there very

heavily. And most certainly, it seems that a lot of the people who went out in to the streets did so because of online mobilization, and that for many of them, it was their first protest action ever, a lot of the people who got detained had never even been at a protest before. And so definitely.

And there were also some Web sites that sort of had kits for people, here is a flier that you can print out and stick up around your neighborhood and so on. And people writing about how, vote for anybody except United Russia. So definitely, both in terms of the protests after the election over what some felt were rigged results as well as the results themselves, it does seem that the Internet played a role.

There were also very aggressive attacks against opposition Web sites as well, and LiveJournal went down, which is kind of one of the most popular blog hosting systems in Russia, and of course, it is hard to pin exact responsibility on who launched the attacks, but people are assuming that the attacks were from people who didn't want the critics of the ruling party to speak out and organize at that time.

Ms. LE COZ. I would like to add that it is specifically because online political debate is really present in Russia that Russia is one of the countries where you can find the most propaganda online because they know it is taking place there, during elections, but also before and after.

And this is a place for political debate. LiveJournal, one of the most popular Web sites goes down every time there is something happening; 15 others that are critical of the actual political situation went down, too. And this is because it is happening there that you have all those attacks.

Mr. PAYNE. Has anyone been monitoring the, in that region, the Ukraine and Belarus? Has there been any, to your knowledge, attack on the Internet or trying to shut it down? Both of those countries are going through some changes right now.

Mr. CALINGAERT. Well, there are actually—Belarus is fairly sophisticated. And in the aftermath of their last Presidential election, where there was significant reports of voter fraud and then protests, and the state-owned Internet service provider was basically redirecting traffic away from opposition Web sites and had created clones, which looked pretty much exactly the same as the original ones, but they had misinformation on them, so they give the wrong place and time of the protests. So there is quite extensive manipulation of the Internet in Belarus and quite sophisticated.

Mr. PAYNE. Well, let me—I also, a statement by the U.S. Government official, I think in a lot of instances sometimes, and I'm not in defense of them because I don't even know who was there, but the government tends to be outmanned it seems in a lot of instances. You will have some staff people there, and you have got the world there with their half-million-dollar lawyers and $200,000 salesmen, and so they overwhelm the, usually, the people there that are supposed to be representing State or the interests of good people. And so, however, I agree that we can't throw in the towel. You can't quit. You have to realize what is happening.

And as we are moving in this, and it is not going to get any better, because as you know, with our debt, and the two things that

are going on—there is a move to even reduce the size of government, so we are going to even have less capability of doing things of this nature when we are getting down to cutting $4 trillion, $5 trillion, $6 trillion over the next 10, 15 years, so the reality is that we are going to have a difficult time if the trend in, at least in the House, continues, so there are going to be some real barriers.

And finally, there is a strong move against regulations. There is another philosophy that regulations stymy growth and we are stagnant in our Nation because we have EPA laws that say we can't pollute; if we could pollute, we could do more coal or something.

So we are going to run into the whole notion of deregulation, and it is going to be even difficult to try to regulate. The battle is going to be to try to hold on to things that are positive in the overall scheme of things. But the argument about growth and jobs tend to be the overriding factor now.

So, I just think, though, that people like those of you here are very essential to this. We will certainly continue to express our views, and I just like to thank all of you for testifying. Thank you.

Mr. SMITH. I would like to thank you, too, for your expertise, your guidance, your wisdom.

Victor Hugo once said, "There is nothing more powerful than an idea whose time has come." This is the year, and it may take a year to get this enacted, but we have got to go and give the tools and empower our own Government to have the ability to restrict these dual-use capable technologies from being used against very fine people who want freedom. And you have provided us tremendous insights, and I thank you so much.

Please, I know you will be there as we move through this process because we are not going to let up until this is law. And I expect we will have huge obstacles in the near term, but at the end of the day, once this is enacted and then we will be talking about reauthorization and improvements in the outer years, people will say, why wasn't that done sooner? So, again, you are long stayers in the fight for human rights. Thank you so much for your insights today and for being here.

The hearing is adjourned.

[Whereupon, at 4:45 p.m., the subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

SUBCOMMITTEE HEARING NOTICE
COMMITTEE ON FOREIGN AFFAIRS
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C. 20515-0128

SUBCOMMITTEE ON AFRICA, GLOBAL HEALTH, AND HUMAN RIGHTS
Christopher H. Smith (R-NJ), Chairman

December 6, 2011

You are respectfully requested to attend an OPEN hearing of the Subcommittee on Africa, Global Health, and Human Rights, to be held in **Room 2172 of the Rayburn House Office Building (and available live, via the WEBCAST link on the Committee website at http://www.hcfa.house.gov):**

DATE: Thursday, December 8, 2011

TIME: 2:00 p.m.

SUBJECT: Promoting Global Internet Freedom

WITNESSES: Daniel Calingaert, Ph.D.
Vice President
Freedom House

Ms. Clothilde Le Coz
Washington Director
Reporters Without Borders

Ms. Elisa Massimino
President and Chief Executive Officer
Human Rights First

Ms. Rebecca MacKinnon
Bernard L. Schwartz Fellow
The New America Foundation

By Direction of the Chairman

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

COMMITTEE ON FOREIGN AFFAIRS

MINUTES OF SUBCOMMITTEE ON *Africa, Global Health, and, Human Rights* HEARING

Day *Thursday* **Date** *December 8, 2011* **Room** *2172 Rayburn*

Starting Time *2:45 p.m.* **Ending Time** *4:45 p.m.*

Recesses *0* (____to ____) (____to ____) (____to ____) (____to ____) (____to ____) (____to ____)

Presiding Member(s)

Rep. Chris Smith

Check all of the following that apply:

Open Session ☑
Executive (closed) Session ☐
Televised ☑
Electronically Recorded (taped) ☑
Stenographic Record ☑

TITLE OF HEARING:

Promoting Global Internet Freedom

SUBCOMMITTEE MEMBERS PRESENT:

Rep. Chris Smith, Rep. Donald Payne, Rep. Ann Marie Buerkle

NON-SUBCOMMITTEE MEMBERS PRESENT: *(Mark with an * if they are not members of full committee.)*

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

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

Prepared statement from Dr. Calingaert
Prepared statement from Ms. Le Coz
Prepared statement from Ms. Massimino
Prepared statement fromMacKinnon
Prepared statement from Rep. Carnahan
Question for the record from Rep. Carnahan
Freedom on the Net report from Freedom House

TIME SCHEDULED TO RECONVENE _____
or
TIME ADJOURNED *4:45 p.m.*

Sheri Rickert
Subcommittee Staff Director

OPENING STATEMENT OF
THE HONORABLE RUSS CARNAHAN (MO-3)
HOUSE FOREIGN AFFAIRS COMMITTEE
SUBCOMMITTEE ON AFRICA, GLOBAL HEALTH, AND HUMAN RIGHTS

Hearing on
Promoting Global Internet Freedom
Thursday, December 8, 2011 2 P.M.
2172 Rayburn House Office Building

Chairman Smith and Ranking Member Payne, thank you for holding this hearing on internet freedom around the world. As internet usage—including social media, blogs, and everyday tasks—has risen rapidly in recent years, this hearing is incredibly important.

The pace and popularity of internet technology has been a powerful tool for freedom of expression and social organization. However, in countries with high restrictions on political dissent, the internet has not only served a forum for information, but as a means for governments to crack down on political and human rights activists.

We have seen this very dichotomy with the Arab uprisings, where social media played a significant role in organizing demonstrations. In response, however, many governments have sought new ways to censor internet content, restrict access, and utilize digital information to identify and monitor opposition.

Promoting internet freedom and strengthening access to our online public diplomacy efforts are a critical component of our democracy promotion and global engagement strategies. I hope to hear more from our witnesses today on the state of internet freedom, particularly in some of the most restrictive countries, like China and Iran, as well as recommendations for the U.S. government, international community, and private sector in response to this method of repression.

In closing, I would like to thank the witnesses for the presence and testimonies here today.

QUESTIONS FOR THE RECORD
THE HONORABLE RUSS CARNAHAN (MO-3)
HOUSE FOREIGN AFFAIRS COMMITTEE
SUBCOMMITTEE ON AFRICA, GLOBAL HEALTH, AND HUMAN RIGHTS

Hearing on
Promoting Global Internet Freedom
Thursday, December 8, 2011 2 P.M.
2172 Rayburn House Office Building

- I would like to turn now to Iran, which Freedom House ranks as the most restrictive country globally. Congress and the Administration have importantly focused on denying the Iranian government's acquisition and deployment of Internet filtering and monitoring tools. Beyond that, the State Department launched a "virtual embassy" in Iran this week. As anticipated, however, it was quickly blocked by the Iranian government. The State department has stated that Iranians can use Virtual Private Networks (VPNs) to access the website, though some are skeptical.
    - What is your understanding of the ability of Iranians to use VPNs and other technology that could enable them to bypass the filtering and monitoring deployed by their government to access information and communicate freely?
    - Are there other viable options to help Iranians and others living in highly restrictive societies circumvent such restricted access?

Freedom House Response to

Questions for the Record from

The Honorable Russ Carnahan

What is your understanding of the ability of Iranians to use VPNs and other technology that could enable them to bypass the filtering and monitoring deployed by their government to access information and communicate freely?

Iranians use a wide range of tools to attempt to access the Internet without censorship. Circumvention tools account for a significant component of the strategy to promote access to information and freedom of expression for Iranian Internet users. These tools each have strengths and weaknesses that potentially influence the users' decision-making process of adoption and use. Users are likely to base their choices on factors such as: availability of the tool, how reliable and fast the connection is, whether the service is perceived as secure, how easy the tool is to use, whether there are costs associated, and how close the tool comes to providing a normal Internet browsing experience. For the purposes of illustration, circumvention tools from the user standpoint can be divided into four categories: 1.) VPNs, 2.) Internet proxies (HTTP/SOCKS Proxy), 3.) Web-based platforms (like Psiphon, Glype) and 4.) Custom software packages (Ultrasurf, Tor, Your-Freedom, Gtunnel, FreeGate, JonDo formerly JAP etc.)

In August 2011, a Freedom House partner on Iran analyzed incoming traffic on two prominent Iranian web sites that are blocked in Iran. It was discovered that prevalence of Virtual Private Networks grew significantly in 2011, despite apparent moves by the government's filtering system to reduce the VPNs' usefulness. Prevalent among the providers seen in our sample were Iranian commercial entities, such as ParsVPN, VPNReactor, VPNServ24, PersianVPN. While the VPN protocol is generally considered cryptographically safe, light auditing would suggest that appropriate attention is not always paid to the server's security, which poses serious concerns. The ease of payment within Iran for the Iranian VPN providers' services points to suspicions that the government is aware of them and likely monitoring their activity. Direct access to foreign commercial VPN providers is limited due to inability to pay for their services.

In comparison to other options provided at no cost, VPNs are fast and more responsive to customer needs. They also appear to scale more quickly, are less susceptible to the dynamics of funding and do not bear the stigma of association with international politics.

The Global Internet Freedom Consortium's tool Ultrasurf (a custom software package identified as GIFC/Dynaweb), takes a good share of circumvention tool usage. Ultrasurf remains a stable and fast method of bypassing the regime's filtering. The software necessary is straightforward, and a Persian-language version is available.

The second group, "internet proxies," includes platforms that serve a moderate number of users, with Your-Freedom, HTTP Tunnels chief among them. Proxies tend not to scale well, and experience congestion issues or abuse by users. Overall, it appears that the role of Internet Proxies have diminished in the past two years, in part due to the labor required to keeping up-to-

date with the latest offerings and ability of Iranian government to observe and block distributed addresses.

Your-Freedom is a commercial German offering that provides tiered levels of access to its network for the purposes of protecting privacy and unrestricted access to information. The free account is limited to 64 kilobits per second, for 15 hours a week, with faster connections offered without time limit for a cost.

HTTP Tunnels are essentially Internet Proxies, although they may require the installation of software to protect user privacy or make more resources available to clients. To improve the user experience of slow Internet connections, these providers will act as intermediaries and compress text and multimedia content – increasing the efficiency of the connection. HTTP Tunnels also allow for browsing sites that would otherwise be restricted due to location licensing, which has the same effect of bypassing filtering by the government.

The third group, "web-based platforms," includes tools that register less than five percent of unique circumvention users. Use of most of these tools involves onerous burdens in terms of network speed, web compatibility or user experience. Some such tools are limited by low public awareness, such as Simurgh e-Sabz. Additionally, some tools appear to have limited the range of websites that can be browsed and, as a result, either do not enjoy wide adoption or do not appear in our population set.

Web-based platforms, such as the Toronto-based Psiphon, are circumvention platforms that operate in the browser, without the installation of any software. Generally, they allow an address to be entered into the website, which will then retrieve the content and display it as though you were on the request page. Since normal web data can be easily monitored, these services often employ SSL-encryption or obfuscation of the content to protect the traffic. Similar to the prior two methods, the method of discovering computers to connect to is not automated and blocking the service is as simple as filtering the domain, keywords or IP address. The publication of new access points is done through web discussion forums and email lists.

Anonymization tools, particularly Tor, provide very strong security assurances, however there is currently a trade-off in speed and stability. We should expect adoption and widespread use primarily in an audience concerned with keeping their identity and traffic masked, rather than among average users.

Developments in the month of February 2012 raised new concerns about Iranian government intentions to further block Internet access in the near future. On February 20, for the second time in two weeks, Internet blockades affected the most common forms of secure connections, including all encrypted international websites outside of Iran that depend on the Secure Sockets Layer protocol (SSL). This action makes services such as Gmail, Facebook and Twitter unavailable to Iranians. Such disruption might be related to upcoming parliamentary voting on March 2 to prevent opposition calls for an election boycott. Widespread blockades, according to prevalent analyses, could be preparation for an insulated national Internet, a project expected to be launched in May/June of 2012. According to Iranian Telecommunications Minister Reza

Taghipour, the project involves creating infrastructure aimed at boosting Iran cyber-defense capabilities.

Are there other viable options to help Iranians and others living in highly restrictive societies circumvent such restricted access?

Our efforts should remain focused on improving the tools discussed above, expanding the pool of similar tools, and educating users about their availability and competing virtues. Other options for circumventing online censorship are available, but do not typically offer the same levels of security and anonymity as those mentioned above. These include satellite-based Internet, mobile Internet, dial-up Internet, and alternate uses of uncensored technology.

While mobile and satellite Internet connections sometimes offer less-censored pathways to Internet content, both modes of communication are subject to monitoring by state authorities. The insecurity of mobile phones is well-documented, and in cases where mobile internet networks are less censored, this may be an indication that a state is permitting this access with the intent of monitoring users. Just this week, the deaths of two Western journalists in Syria raised new concerns about the security of satellite-based connections: there is strong evidence that the Syrian government identified their location and targeted them based on their satellite connections.

Dial-up Internet, generally considered an obsolete technology, sometimes, as a result, avoids the same censorship as broadband networks. However, these connections are fundamentally insecure, and cannot be trusted to protect the privacy of any communications.

Uncensored network technologies can sometimes be repurposed by those seeking to connect beyond a national firewall. In many online games, for example, a chat or voice interface will allow users to bypass censorship and communicate across borders. Likewise Dropbox, an online data backup service, can sometimes be used to transfer files past firewalls.

In general, once users find a circumvention tool with which they are comfortable, they tend to stay with that tool. Among VPN users, for example, only 15 percent turned to another service during our research period, and less than one-half of one percent had used more than two. As such, outreach and promotion should direct users toward those tools that offer a reliable level of security and anonymization, such as Tor, Psiphon, and others discussed above.

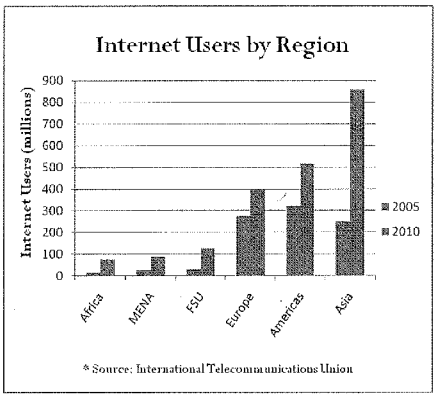
Technical and security circumstances vary greatly from country to country, as do political and legal contexts. What is a reliable and safe circumvention tool in Vietnam may be dangerously insecure in a place like Syria. Country-specific circumstances vary greatly and should always be taken into account when offering guidance to users and setting priorities for tool development.

NEW TECHNOLOGIES, INNOVATIVE REPRESSION: Growing Threats to Internet Freedom

By Sanja Kelly and Sarah Cook

Over the past decade, and particularly in the last few years, the influence of the internet as a means to spread information and challenge government-imposed media controls has steadily expanded. This mounting influence directly corresponds to the growth in the number of users around the world: over two billion people now have access to the internet, and the figure has more than doubled in the past five years. However, as more people use the internet to communicate, obtain information, socialize, and conduct commerce, governments have stepped up efforts to regulate, and in some instances tightly control, the new medium. Reports of website blocking and filtering, content manipulation, attacks on and imprisonment of bloggers, and cyberattacks have all increased sharply in recent years.

To illuminate the nature of the emerging threats and identify areas of growing opportunity, Freedom House has conducted a comprehensive study of internet freedom in 37 countries around the globe. An earlier, pilot version was published in 2009, covering a sample of 15 countries. The new edition, *Freedom on the Net 2011*, assesses a wider range of political systems, while tracking improvements and declines in the countries examined two years ago. Over 40 researchers, most of whom are based in the countries they examined, contributed to the project by researching laws and practices relevant to the internet, testing accessibility of select websites, and interviewing a wide range of sources. Although the study's findings indicate that the threats to internet freedom are growing and have become more diverse, they also highlight a pushback by citizens and activists who have found ways to sidestep some of the restrictions and use the power of new internet-based platforms to promote democracy and human rights.



When the internet first became commercially available in the 1990s, very few restrictions on online communications and content were in place. Recognizing the economic potential of the new medium, many governments started investing heavily in telecommunications infrastructure, and internet-service providers (ISPs) sought to attract subscribers by creating online chat rooms and building communities of users around various topics of interest. Even the authorities in China, which today has the most sophisticated regime of internet controls, exerted very little oversight in the early days. However, as various dissident groups in the late 1990s began using the

internet to share information with audiences inside and outside the country, the government devoted tremendous human and material resources to the construction of a multilayered surveillance and censorship apparatus. Although China represents one of the most severe cases, similar dynamics are now becoming evident in many other countries.

Indeed, the country reports and numerical scores in this study reveal that a growing number of governments are moving to regulate or restrict the free flow of information on the internet. In authoritarian states, such efforts are partly rooted in the existing legal frameworks, which already limit the freedom of the traditional media. These states are increasingly blocking and filtering websites associated with the political opposition, coercing website owners into taking down politically and socially controversial content, and arresting bloggers and ordinary users for posting information that is contrary to the government's views. Even in more democratic countries—such as Brazil, India, Indonesia, South Korea, Turkey, and the United Kingdom—internet freedom is increasingly undermined by legal harassment, opaque censorship procedures, or expanding surveillance. The spread and intensification of internet controls in each country that showed decline generally conformed to one of the following three patterns:

Initial signs of politically motivated internet controls: In several countries that were previously free from most internet controls, the first signs of politicized censorship and user rights violations emerged, often in the period before or during elections. Many of these incidents represented the first time that a website in the country had been blocked, a user detained, or a restrictive law passed. This dynamic was particularly evident in Venezuela, Azerbaijan, Jordan, and Rwanda. In Venezuela, for example, users subscribing to internet services through the state-owned telecommunications firm CANTV reported that they were unable to access opposition-oriented blogs and a popular news site in the days surrounding parliamentary elections in September 2010. In Azerbaijan in 2009, the authorities temporarily blocked several websites that lampooned the president, and jailed two youth activists who posted a video that mocked the government.

Acceleration and institutionalization of internet controls: In countries where the authorities had already shown some tendency toward politically motivated controls over the internet, the negative trend accelerated dramatically, and new institutions were created specifically to carry out censorship. In Pakistan, for example, where temporary blocks have been common in recent years, a new Inter-Ministerial Committee for the Evaluation of Websites was established in mid-2010 to flag sites for blocking based on vaguely defined offenses against the state or religion. In Thailand, the government has long blocked internet content and taken legal action against users, particularly those posting information that is critical of the monarchy. However, the number of detained offenders and blocked sites sharply increased over the last two years, particularly while top officials had the authority to extrajudicially order blockings under a state of emergency that lasted from April to December 2010.

Strengthening of existing internet-control apparatus: Even in countries with some of the most robust censorship and internet surveillance systems in the world, measures were taken to eliminate loopholes and further strengthen the apparatus. In China, blogs on political and social issues were shut down, the space for anonymous communication has dwindled, and the

government has stepped up efforts to counter circumvention tools. In Bahrain, Iran, Ethiopia, and Tunisia, intensified censorship or user arrests came in the context of popular protests or contentious elections. Following the June 2009 elections in Iran, the country's centralized filtering system evolved to the point of being able to block a website nationwide within a few hours, and over 50 bloggers have been detained. In Vietnam, in addition to blocking websites, restricting some social-networking tools, and instigating cyberattacks, the authorities displayed their muscle by sentencing four activists to a total of 33 years in prison for using the internet to report human rights violations and express prodemocracy views.

The new internet restrictions around the globe are partly a response to the explosion in the popularity of advanced applications like Facebook, YouTube, and Twitter, through which ordinary users can easily post their own content, share information, and connect with large audiences. While mostly serving as a form of entertainment, over the last two years these tools have also played a significant role in political and social activism. In Egypt and Tunisia, for example, democracy advocates have relied heavily on Facebook to mobilize supporters and organize mass rallies. Similarly, Bahraini activists have used Twitter and YouTube to inform the outside world about the government's violent response to their protests. Even in Cuba, one of the most closed societies in the world, several bloggers have been able to report on daily life and human rights violations.

Many governments have started specifically targeting these new applications in their censorship campaigns. In 12 of the 37 countries examined, the authorities consistently or temporarily imposed total bans on YouTube, Facebook, Twitter, or equivalent services. Moreover, the increased user participation facilitated by the new platforms has exposed ordinary people to some of the same punishments faced by well-known bloggers, online journalists, and human rights activists. Among other recent cases, a Chinese woman was sent to a labor camp over a satirical Twitter message, and an Indonesian housewife faced high fines for an e-mail she sent to friends complaining about a local hospital. Because new technologies typically attract the young, some of those arrested have been teenagers, including an 18-year old Iranian blogger writing about women's rights and a 19-year old Tibetan detained after looking at online photographs of the Dalai Lama.

In 23 of the 37 countries assessed, a blogger or other internet user was arrested for content posted online.

KEY FINDINGS

The 2011 edition of *Freedom on the Net* identifies a growing set of obstacles that pose a common threat to internet freedom in many of the countries examined. Of the 15 countries covered in the pilot, a total of 9 registered score declines over the past two years. The newly added countries lack earlier scores for comparison, but conditions in at least half of them suggest a negative trajectory, with increased government blocking, filtering, legal action, and intimidation to prevent users from accessing unfavorable content. In cases where these tactics are deemed ineffective or inappropriate, authorities have turned to cyberattacks, misinformation, and other indirect methods to alter the information landscape.

Political Content Increasingly Blocked, Transparency Lacking

Governments around the world have responded to soaring internet penetration rates and the rise of user-generated content by establishing mechanisms to block what they deem to be undesirable information. In many cases, the censorship targets content involving illegal gambling, child pornography, copyright infringement, or the incitement of hatred or violence. However, a large number of governments are also engaging in deliberate efforts to block access to information related to politics, social issues, and human rights.

Of the 37 countries examined, the governments of 15 were found to engage in substantial blocking of politically relevant content. In these countries, instances of websites being blocked are not sporadic or limited in scope. Rather, they are the result of an apparent national policy to restrict users' access to dozens, hundreds, or most often thousands of websites, including those of independent and opposition news outlets, international and local human rights groups, and individual blogs, online videos, or social-networking groups.

Countries with substantial censorship of political or social issues in 2009–10:

Bahrain, Belarus, Burma, China, Cuba, Ethiopia, Iran, Kazakhstan, Pakistan, Saudi Arabia, South Korea, Thailand, Tunisia, Turkey, Vietnam

Website blocking is typically implemented by ISPs acting on instructions from a government agent, judge, or other appointed entity, whose orders may apply to a particular domain name, an internet-protocol (IP) address, or a specific URL. ISPs keep track of and periodically receive updates on the resulting blacklists of banned sites. In a small number of countries, the filtering technology employed is more sophisticated, and can scan users' browsing requests for certain banned keywords. Keyword filtering is much more nuanced, enabling access to a given website but not to a particular article containing a sensitive keyword in its URL path. Among the countries studied, China, Iran, and Tunisia are known to have such systems in place. In China, which boasts the world's most comprehensive censorship apparatus, keyword filtering is evident in instant-messaging services as well, having been built into the software of popular messaging programs like TOM Skype and QQ.

Two of the countries categorized by Freedom House as electoral democracies—Turkey and South Korea—were also found to engage in substantial political censorship. In Turkey, a range of advanced web applications were blocked, including the video-sharing website YouTube, which was not accessible in Turkey from May 2008 to October 2010. South Korean authorities blocked access to an estimated 65 North Korea–related sites, including the official North Korean Twitter account, launched in August 2010. Meanwhile, the governments of Australia, Indonesia, and Italy introduced proposals that would enable automated filtering by ISPs, create a state-led multimedia content screening entity, and extend prescreening requirements from television broadcasting to video-hosting websites, respectively. By the end of 2010, these proposals had been set aside or amended to remove the most egregious requirements.

One aspect of censorship was evident across the full spectrum of countries studied: the arbitrariness and opacity surrounding decisions to restrict particular content. In most nondemocratic settings, there is little government effort to inform the public about which content is censored and why. In many cases, authorities avoid confirming that a website has been

deliberately blocked and instead remain silent or cite "technical problems." Saudi Arabia does inform users when they try to access a blocked site, and the rules governing internet usage are clearly articulated on government portals, but as in many countries, the Saudi authorities often disregard their own guidelines and block sites at will. Even in more transparent, democratic environments, censorship decisions are often made by private entities and without public discussion, and appeals processes may be onerous, little known, or nonexistent.

The widespread use of circumvention tools has eased the impact of content censorship and at times undermined it significantly. Such tools are particularly effective in countries with a high degree of computer literacy or relatively unsophisticated blocking techniques. For example, YouTube remained the eighth most popular website among Turkish users despite being officially blocked in that country for over two years, and the number of Vietnamese Facebook users doubled from one to two million within a year after November 2009, when the site became inaccessible by ordinary means. Users need special skills and knowledge to overcome blockages in countries such as China and Iran, where filtering methods are more sophisticated and the authorities devote considerable resources to limiting the effectiveness of circumvention tools. Still, activists with the requisite abilities managed to communicate with one another, discuss national events in an uncensored space, and transmit news and reports of human rights abuses abroad.

Cyberattacks Against Regime Critics Intensify

Some governments and their sympathizers are increasingly using technical attacks to disrupt activists' online networks, eavesdrop on their communications, and cripple their websites. Such attacks were reported in at least 12 of the countries covered in this study. However, attacks perpetrated by nonstate actors for ordinary criminal purposes are also a growing problem, particularly as internet penetration deepens and more users turn to the medium for shopping, banking, and other activities.

China has emerged as a major global source of cyberattacks. Although not all attacks originating in the country have been explicitly traced back to the government, their scale, organization, and chosen targets have led many experts to conclude that they are either sponsored or condoned by Chinese military and intelligence agencies. The assaults have included denial-of-service (DoS) attacks on domestic and overseas human rights groups, e-mail messages to foreign journalists that carry malicious software capable of spying on the recipient's computer, and large-scale hacking raids on the information systems of over 30 financial, defense, and technology companies, most of them based in the United States. In addition, independent analysts have detected cyberespionage networks that extend to 103 countries as part of an effort to spy on the Tibetan government-in-exile and its foreign government contacts.

As with offline forms of violence and intimidation, governments seem most likely to resort to cyberattacks when their power is threatened by disputed elections or some other political crisis. In Iran, for example, during the mass protests that followed the June 2009 presidential election, many opposition news sites were disabled by intense DoS attacks, and there is technical evidence confirming that government-owned IP addresses were used to launch the assaults. A group calling itself the Iranian Cyber Army, which operates under the command of the Islamic Revolutionary

Guard Corps, managed to hack a number of other sites with a mix of technical methods and forgery.

Similarly, in the wake of fraudulent elections in Belarus in December 2010, the government initiated DoS attacks against opposition websites, dramatically slowing down their connections and in some instances rendering them completely inaccessible. Belarusian authorities also engaged in a type of web forgery designed to confuse users and provide false information. For example, the country's largest ISP, the state-owned Belpak, redirected users from independent media sites to nearly identical clones that provided misleading information, such as the incorrect location of a planned opposition rally.

Countries where websites or blogs of government opponents faced cyber attacks in 2009-2010:

Bahrain, Belarus, Burma, China, Iran, Kazakhstan, Malaysia, Russia, Saudi Arabia, Thailand, Tunisia, Vietnam

The Tunisian regime of President Zine al-Abidine Ben Ali accelerated its hacking activity in the run-up to the January 2011 uprising that drove it from power. Security officials regularly broke into the e-mail, Facebook, and blogging accounts of opposition and human rights activists, either deleting specific material or simply collecting intelligence about their plans and contacts.

Governments Increasingly Exploit Centralized Infrastructure and Built-In Internet Chokepoints

Although it often goes largely unnoticed, centralized government control over a country's connection to international internet traffic poses a significant threat to online free expression and privacy, particularly at times of political turmoil. In about a third of the states examined, the authorities have exploited their control over infrastructure to limit widespread access to politically and socially controversial content, or in extreme cases, to cut off access to the internet entirely.

This centralization can take several forms. In Ethiopia and Cuba, for example, state-run telecommunications companies hold a monopoly on internet service, giving them unchecked control over users' ability to communicate with one another and the outside world. Elsewhere, the state-run company's control of the market is not complete, but its dominance is sufficient to significantly influence people's access to information. Thus when CANTV in Venezuela or Kazakhtelecom in Kazakhstan block a website, it becomes inaccessible to the vast majority of internet users.

As a growing number of governments liberalize the ISP market, such centralization may become less obvious. In countries including Egypt and Belarus, a state-controlled company owns the country's network of copper wires or fiber-optic cables and sells bandwidth downstream to a variety of retail-level ISPs. In China, Vietnam, and Saudi Arabia, an array of three to eight international gateways are available to multiple, economically competitive ISPs, yet ultimate control over the country's connectivity rests with the government.

Of the 37 countries assessed, 19 had at least a partially centralized and government-controlled international connection. Authorities in at least 12 of these were known to have used their leverage to restrict users' access to politically relevant information or engage in widespread

surveillance. Egypt joined the list in January 2011, when officials shut down the internet nationwide for five days in an unsuccessful attempt to curb antigovernment protests. Technicians reportedly cut off almost all international traffic flowing through a tiny number of portals, while ISPs, particularly state-owned Telecom Egypt, removed the routes to Egypt's networks from global routing tables—the mechanism that provides pathways for users' computers to connect to requested websites. The operation was accomplished within the span of one hour.

The Egyptian case demonstrates that at times of political unrest, authoritarian leaders do not hesitate to exploit infrastructural controls to protect their rule, even if it causes massive disruptions to economic activity and personal communications. Several other instances of this "kill switch" phenomenon have occurred in recent years. In 2007, at the height of a wave of popular protests led by Buddhist monks in Burma, state-run ISPs cut off the country's internet connection from September 27 to October 4. More recently, from July 2009 to May 2010, the Chinese authorities severed all connections to the northwestern region of Xinjiang while security forces carried out mass arrests in the wake of ethnic violence. Local government websites and other content hosted within Xinjiang remained accessible, but the region's 20 million residents were cut off from outside information and a range of services used daily by individuals and businesses—including e-mail, instant messaging, and blog-hosting.

Countries with at least partially centralized and government-controlled internet connections:

Azerbaijan, Bahrain, Belarus, Burma, China, Cuba, Egypt, Ethiopia, Iran, Jordan, Kazakhstan, Malaysia, Saudi Arabia, Thailand, Tunisia, Turkey, Venezuela, Vietnam, Zimbabwe

In addition to outright shutdowns, a centralized, state-controlled internet infrastructure facilitates two other types of restrictions: the deliberate slowing of connection speeds and the imposition of a nationwide system of filtering and surveillance. During opposition protests in Iran in the summer of 2009, authorities sharply reduced the speed of network traffic, making it difficult to conduct basic online activities like opening e-mail messages. Uploading a single image could take up to an hour. In early 2011, as protests began flaring up across the Middle East, the Bahraini government selectively slowed down internet connections at newspaper offices, hotels, and homes. The prime example of a centralized filtering system is China's so-called Great Firewall, but other countries, including Iran and Saudi Arabia, also use such systems to enforce nationwide censorship and monitor dissident activity.

Offline Coercion, Online Manipulation Alter Available Information

Rather than relying exclusively on technological sophistication to control internet content, many governments employ cruder but nevertheless effective tactics to delete and manipulate politically or socially relevant information. These methods are often ingenious in their simplicity, in that their effects are more difficult to track and counteract than ordinary blocking.

One common method is for a government official to contact a content producer or host, for example by telephone, and request that particular information be deleted from the internet. In some cases, individual bloggers or webmasters are threatened with various reprisals should they refuse the request. Increasingly, governments and their supporters are also taking advantage of

international hosting platforms' complaint mechanisms to have user-generated content removed. Over the past two years, activists from China, Egypt, Ethiopia, Mexico, and Tunisia found that their YouTube videos or Facebook accounts had been removed or disabled after complaints were filed, apparently by regime supporters. In several of these instances, the content was restored once the problem was brought to the hosting company's attention, but the threat of a blanket ban is sometimes enough to induce large websites to meet governments' specific deletion demands.

A certain set of countries have laws in place to hold content providers and hosts legally responsible for what others post on their sites. Such provisions effectively force the site owner to screen all user-generated content and delete what might be deemed offensive by the authorities. Long-standing laws in China have led internet companies there to employ hundreds of thousands of people responsible for monitoring and censoring online videos, bulletin-board discussions, blog posts, and microblog messages. Nevertheless, in 2009 and 2010, the Chinese authorities adopted various measures to increase pressure on private websites, obliging them to be more vigilant and prevent content from slipping through the cracks. In Thailand, Kazakhstan, Vietnam, and Venezuela, new laws or directives promulgated since 2007 have led to an increase in this type of censorship. In Thailand, for instance, online news outlets are legally responsible for comments posted by readers, and at least one editor is facing criminal charges over reader comments that were critical of the monarchy. In Vietnam and Venezuela, some webmasters and bloggers have disabled the comment feature on their sites to avoid potential liability.

In addition, a range of governments have deployed manpower and resources to proactively manipulate online discussion and bolster progovernment views. Thailand has military units assigned to countering online criticism of the monarchy, and Burma has established a blogging committee in each ministry. Elsewhere, those recruited and paid for such tasks may be ordinary citizens, often youth. Thus China has cadres, known as the "50 Cent Party" for their supposed per-comment fees, who are employed to post progovernment remarks on various online forums, and recruiting advertisements for similar commentators have reportedly begun to appear on Russian job sites. Government-sponsored posts aim not only to defend the leadership and its policies, but also to discredit opposition voices or human rights activists, and to deceive everyday users. During postelection protests in Iran, for example, government supporters posted fake user-generated content to Twitter and YouTube to mislead protesters and journalists.

In a somewhat different manipulation technique, search-engine providers in some countries, most notably China, are required to adjust search results to match government-imposed criteria, for instance by only offering government-affiliated sources on particular topics. In addition to displeasure over a series of cyberattacks, this obligation was at the center of Google's decision to withdraw from China in early 2010.

This section is an excerpt from Freedom House's Freedom on the Net 2011 report.

The complete report can be accessed at:
http://freedomhouse.org/sites/default/files/FOTN2011.pdf

OVERVIEW: NEW TECHNOLOGIES, INNOVATIVE REPRESSION

[NOTE: The previous report is not reprinted in its entirety but is available in committee records.]

○