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."