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.