REPORTERS WITHOUT BORDERS
FOR PRESS FREEDOM

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 New*s 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.