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.