Statement for the Record of Leslie Harris
President/CEO, Center for Democracy & Technology
Before the Senate Judiciary Committee,
Subcommittee on Human Rights and the Law

"Global Internet Freedom: Corporate Responsibility and the Rule of Law"

May 20, 2008

Chairman Durbin and Members of the Subcommittee:

The Center for Democracy & Technology ("CDT") applauds the Subcommittee's leadership in addressing the growing threat of state-sponsored censorship and surveillance of the Internet, and we appreciate the opportunity to submit this written testimony.

CDT's core mission is to advocate for public policies, standards and industry practices that keep the Internet open, innovative and free. We believe that an open Internet can be a powerful tool for human rights and democracy. It can facilitate government accountability and transparency, allowing citizens to pierce through official propaganda and access vast alternative sources of information. The Internet is a uniquely decentralized "end to end" network, which places power in the hands of users rather than with gatekeepers in the middle. It permits anyone with a connection to speak, advocate for political freedom and collaborate with others. It has been 60 years since the Universal Declaration of Human Rights first articulated a broad right to freedom of expression regardless of borders.1 The Internet offers a unique promise to fulfill that vision.

Because of its openness and low barriers to entry, the Internet is a uniquely disruptive technology to repressive regimes and its global deployment presents an unprecedented challenge to governments that seek to tightly control the flow of ideas and information within their borders. Trade liberalization and the lure of the global markets have made participation in the global Internet an imperative even for

---

[1] Article 19, Universal Declaration of Human Rights (1948), http://www.un.org/Overview/rights.html.

many repressive governments. The challenge as they see it is to harness the Internet's power for economic growth while limiting its freedoms.2

The task of controlling such a highly distributed network is not an easy one. As the numbers of users increase along with the sheer number of devices that connect to the Internet, the ability to control what people do and see online diminishes and the threat to totalitarian governments escalates. Some countries, including China, have responded with an elaborate censorship and surveillance apparatus,3 while other governments simply encourage citizens' self-censorship by spreading rumors of the existence of such monitoring.4 In other countries, Internet access itself is limited or banned outright.5

Increasingly, repressive regimes are turning to Internet companies and other technology intermediaries to assist with censorship and surveillance. Global technology companies are increasingly faced with a Hobson's choice: follow the law of the countries in which they offer services and risk participating in human rights violations, or refuse to cooperate and risk loss of a business license and the right to provide services in that country. In CDT's view, neither result serves the goal of Internet freedom.

While there is no easy answer to the rise of Internet repression, we strongly believe that the United States government must play a decisive role and use the instruments at its disposal including diplomacy, trade policy, and foreign aid to advocate for Internet freedom. We further urge the U.S. government to work collaboratively with U.S. technology companies to help them better identify and manage the risks posed by providing Internet services or selling sensitive technologies in high-risk countries.

Companies, too, have a duty to take actions that protect the free expression and privacy rights of their users. Companies must engage in rigorous due diligence and risk assessment when entering difficult markets to identify human rights risks and integrate the protection of human rights into all relevant aspects of their operations. As we discuss further below, CDT also believes that an accountable set of

---

[2] China, for example, wants the economic growth and world recognition that comes with hosting the Olympics but refuses to grant the media and Internet freedom that should rightly accompany it. *See* Ben Blanchard, "China won't guarantee Web freedom over Olympics," *Reuters* (May 8, 2008) http://www.reuters.com/article/reutersComService_2_MOLT/idUSPEK14583520080508.

[3] *See, generally*, Human Rights in China, http://www.hrichina.org/public/. *See also* OpenNet Initiative's China profile: http://opennet.net/research/profiles/china.

[4] *See* OpenNet Initiative's discussion of "induced self-censorship": http://opennet.net/about-filtering.

[5] *See, e.g.*, the OpenNet Initiative's analysis of the Burmese government's shut down of the Internet during fall 2007 following massive protests: "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma," http://opennet.net/research/bulletins/013.

voluntary industry principles can help companies chart an ethical path forward and resist abusive censorship and surveillance demands by governments.

Congress and the Executive Branch should make global Internet freedom a top human rights and foreign policy priority.

Congress has an important role to play in ensuring that Internet freedom is fully incorporated into United States human rights and foreign policy and that it is a central focus of diplomacy, trade and foreign aid. Especially where, as in the case of Internet freedom, many countries are failing to live up to their human rights obligations, the United States and other democratic nations have a duty to act.6 Both Congress and the Executive Branch should make Internet freedom a top human rights and foreign policy priority. The State Department should monitor and report on threats to Internet freedom and should fully incorporate the issue into its diplomatic efforts in all relevant forums.

Congress should also consider how progress toward Internet freedom could be factored into the criteria for development assistance and the conditions for new trade agreements.7 We believe that Internet censorship should be treated as a trade barrier in appropriate circumstances – initial steps have been taken in the European Union toward adoption of this approach and it has been discussed in U.S. policy circles.8 It is also appropriate for Congress to direct that there be an examination of whether narrowly targeted export restrictions are necessary when technology, equipment or expertise is specifically designed for surveillance or censorship.9

---

[6] It is important to note that the United States has ratified or signed key human rights treaties, including the International Covenant on Civil & Political Rights, http://www.unhchr.ch/tbs/doc.nsf/newhvstatusbycountry?OpenView&Start=1&Count=250&Expand=187#187

[7] For example, the Foreign Assistance Act could be amended to include Internet freedom as an explicit factor to be considered when allocating development assistance. *See* 22 U.S.C. § 2151n(c). Additionally, Congress annually appropriates money to help fund the Millennium Challenge Account, managed by the President's Millennium Challenge Corporation, and could ensure that these funds are used to advance Internet freedom in country grantees. For Fiscal Year 2008, while "freedom of expression" is a factor in both the Civil Liberties Indicator and the Voice and Accountability Indicator, Internet freedom – both online freedom of expression and privacy of digitized personal information – are not explicit factors: *Guide to the MCC Indicators and Selection Process, Fiscal Year 2008*, http://www.mcc.gov/documents/mcc-fy08-guidetoindicatorsandtheselectionprocess.pdf.

[8] *See* Eric Bangeman, "EU may begin treating 'Net censorship as a trade barrier," *Ars Technica* (Feb. 27, 2008), http://arstechnica.com/news.ars/post/20080227-eu-may-begin-treating-net-censorship-as-a-trade-barrier.html. *See also* "A Framework for Global Electronic Commerce" (July 1997), http://www.w3.org/TR/NOTE-framework-970706.html#content.

[9] *See, e.g*, Keith Bradsher, "At Trade Show, China's Police Shop for the West's Latest," *New York Times* (April 26, 2008) (noting that the Commerce Department's crime control export regulations "paid little attention to the rising computer industry and have not been updated."), http://www.nytimes.com/2008/04/26/business/worldbusiness/26security.html. *See also* Naomi Klein, "China's All-Seeing Eye: With the help of U.S. defense contractors, China is building the prototype for a high-tech police state. It is ready for export," *Rolling Stone* (May 29, 2008), http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye/.

Finally, we strongly support the statutory creation of an Office of Global Internet Freedom in the Department of State, which would serve as the focal point for mobilizing the tools of U.S. diplomacy and policy in furtherance of online freedom of expression and privacy, and which would institutionalize and continue the work of the Global Internet Freedom Task Force (GIFT) created by the State Department in 2006.10

The steps that we outline are simple and straightforward, but achieving them may be easier said than done. There is considerable "policy incoherence" between the United States' positions on human rights and its policies on trade and foreign aid.11 For example, the U.S. government has conferred "most-favored nation" trade status on countries such as China and Vietnam,12 which have poor human rights records and engage in pervasive Internet surveillance and censorship. The U.S. government also provides significant aid to countries that are key allies in the "war on terrorism" such as Pakistan13 and Egypt,14 but that also have poor human rights records and spotty records on Internet freedom. If Congress decides to elevate the importance of Internet freedom in foreign policy and trade (as we think it should), then it will be critical that such mandates be implemented in a manner that is even-handed and coherent.

Furthermore, the United States and other democratic countries must show their commitment to Internet freedom by carefully guarding Internet freedom at home. Democratic countries have been increasingly turning to content blocking and

---

[10] http://www.state.gov/g/drl/rls/78340.htm.

[11] The UN Special Representative on business and human rights provides a useful discussion of "horizontal policy incoherence" where a government's policies on such things as "trade, investment promotion, development, [and] foreign affairs – work at cross purposes with stated human rights policies and obligations and the agencies charged with implementing them." John Ruggie, *Protect, Respect and Remedy: a Framework for Business and Human Rights*, at 11-14 (April 7, 2008), http://www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf.

[12] George W. Bush, Normal Trade Relations Treatment Executive Order [China] (Dec. 27, 2001), http://www.whitehouse.gov/news/releases/2001/12/20011227-1.html; Proclamation To Extend Nondiscriminatory Treatment (Normal Trade Relations Treatment) to the Products of Vietnam (Dec. 29, 2006), http://www.whitehouse.gov/news/releases/2006/12/20061229-7.html.

[13] According to Reporters Without Borders, "The United States has given the Pakistani intelligence services much technological help to monitor online traffic and it has played a major role in arresting terrorists," http://www.rsf.org/article.php3?id_article=10794. *See also* David Rohde, et al., "U.S. Officials See Waste in Billions Sent to Pakistan," *New York Times* (Dec. 24, 2007), http://www.nytimes.com/2007/12/24/world/asia/24military.html?ex=1356152400&en=19a8b44eb685fafa&ei=5088&partner=rssnyt&emc=rss. *See also* OpenNet Initiative's report on Pakistan's Internet filtering: http://opennet.net/research/profiles/pakistan.

[14] *See, e.g.*, Issandr El Amrani, "Cashing in on the war on terrorism: In exchange for its support since Sept. 11, Egypt has received billions in international aid and diminished scrutiny of its human rights abuses," Salon.com (Feb. 13, 2002), http://dir.salon.com/story/news/feature/2002/02/13/egypt/. See also "Egypt blogger jailed for 'insult'," BBC News (Feb. 22, 2007), http://news.bbc.co.uk/2/hi/middle_east/6385849.stm; Ellen Knickmeyer, "Fledgling Rebellion on Facebook Is Struck Down by Force in Egypt," Washington Post (May 18, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/05/17/AR2008051702672.html.

other Internet speech restrictions, for example, to address social ills.15 Moreover, since 9/11, both the U.S. and Western Europe have taken steps that make it easier to spy on the activities of Internet users and access personal information, setting a poor example that repressive countries are quick to cite in support of their own surveillance.16 While it is not our intention here to debate the merits of particular U.S. domestic policies, there is little doubt that activities such as the NSA's illegal warrantless wiretapping of Americans' electronic communications and the alleged involvement of U.S. companies in that effort have weakened our position as the standard bearer of Internet freedom.17

The technology industry must exercise due diligence in order to minimize human rights risk.

As the global technology industry pursues new markets, it is increasingly confronted with government demands to censor Internet content and turn over information on users in circumstances that place human rights at risk. Most often, these activities are a condition of doing business in a country. Companies have struggled to find an ethical path forward, sometimes pushing back or finding ways to skirt the edges of vague censorship mandates in order to make more information available to users, and other times stumbling badly and inadvertently facilitating human rights violations.18 While some argue that technology companies should simply withdraw from challenging markets, most Internet freedom advocates agree with CDT that the presence of the U.S. Internet industry – and the communications and information services they provide – plays an important role in expanding global Internet freedom.

---

[15] *See* OpenNet Initiative's analysis of North America's and Europe's voluntary and legally mandated restrictions on Internet speech: http://opennet.net/research/regions/namerica; http://opennet.net/research/regions/europe.

[16] For example, there has been an ongoing battle in Congress over whether to legitimize NSA warrantless wiretapping of Americans' electronic communications and immunize the complicit telecommunications companies. *See* House Judiciary Committee hearing on Sept. 5, 2007: http://judiciary.house.gov/oversight.aspx?ID=367, and Sept. 18, 2007: http://judiciary.house.gov/oversight.aspx?ID=370; and Senate Judiciary Committee hearing on Oct. 31, 2007: http://judiciary.senate.gov/hearing.cfm?id=3009. Also, the Justice Department has sought to expand the Communications Assistance for Law Enforcement Act ("CALEA") to reach the Internet, and thereby impose burdensome surveillance technology mandates onto online service providers. *See American Council on Education v. Federal Communications Commission*, 451 F.3d 226 (D.C. Cir. 2006). Similarly, the European Union and Western European countries have been stepping up surveillance capabilities and have imposed new requirements for data retention. *See, e.g.*, "German court allows limited Internet surveillance," *AFP* (Feb. 27, 2008), http://afp.google.com/article/ALeqM5h3zO5qr1MexZtdmJMTdOTVsOVjcg; and the EU's directive on data retention (March 15, 2006): http://register.consilium.europa.eu/pdf/en/05/st03/st03677-re12.en05.pdf.

[17] *See* "The Slippery Slope of Web Censorship," *ABCNews.com* (Oct. 25, 2007), http://abcnews.go.com/Technology/story?id=3771510&page=1.

[18] *See* Human Rights Watch, *Race to the Bottom: Corporate Complicity in Chinese Internet Censorship* (Aug. 2006), http://www.hrw.org/reports/2006/china0806/china0806web.pdf.

Having said that, the question remains: What should be the obligations of these companies with respect to human rights and how should those obligations be effectuated? There is little doubt that companies are also human rights actors. As the UN special representative on business and human rights has concluded, while "their responsibilities cannot and should not mirror the duties of States," companies do have an obligation to respect human rights – and that duty is not "passive" but rather must entail "positive steps."19 The UN special representative on business and human rights, John Ruggie, set forth a thoughtful framework for corporate action and public policy that centers on the exercise of "due diligence" and the identification and management of human rights risk. As Ruggie explains, the corporate responsibility to respect human rights must be embraced at the highest levels of a company and must be incorporated into all aspects of operations. "Due diligence," specifically, requires:

- Rigorous identification of human rights risks posed by a country context, the company's activities within that context, and the activities of its business partners and suppliers;
- Development and implementation of a proactive plan to minimize or eliminate human rights risks; and
- Ongoing monitoring and auditing to track performance and refine practices.[20]

The due diligence approach outlined in the Ruggie report will not produce binary rules that apply to all companies in all circumstances nor will it ensure that mistakes will never occur. The technology sector will continue to have to navigate between the demands of domestic law and their obligation to respect human rights. But the sector will be better equipped to make responsible decisions about which products and services should be offered in a particular market and to build in safeguards for respecting human rights into all aspects of their operations.

The technology industry should adopt voluntary principles to guide its conduct.

While it is incumbent on each company facing demands for abusive filtering and surveillance to engage in due diligence as described above, CDT strongly believes that collective action will strengthen individual company efforts. In our view, the most promising path forward is a set of robust voluntary industry

[19] Ruggie report, *supra* note 11, at 16-17.

[20] Ruggie report, *supra* note 11, at 17-19. Similarly, the London-based International Business Leaders Forum (IBLF) has created a comprehensive human rights risk assessment model, with eight discreet steps companies should take, which has been "road-tested" over the past year, http://www.iblf.org/resources/general.jsp?id=123946.

principles, developed in concert with human rights groups and other key stakeholders, and widely adopted as a global industry standard.

For the past 18 months, CDT has had the privilege of co-facilitating an important multi-stakeholder initiative to develop voluntary principles to guide the Internet and telecommunications industry response to the growing challenges to online free expression and privacy. Both U.S. and European companies have been participating, as have major human rights and press freedom groups, leading academic institutions and social investment funds.[21]

By agreement of all parties, the process has been highly confidential in order to build trust and encourage a candid exchange of ideas and information. For that reason, I cannot discuss the substance of the principles or the supporting accountability and governance documents, all of which are in draft form. I can say, however, that this process has been taken very seriously by all participants and has already led to new thinking and practices among some of the companies involved. And while there are still important issues to resolve, I am hopeful that we are close to reaching our goal. If we succeed, I am confident that the results will begin to provide an ethical and accountable path forward for the companies at the table, arming them to better respond to human rights challenges. I am also hopeful that we will sow the seeds of a global industry standard and create a powerful forum for shared learning and collaborative action between the companies and other stakeholders, including like-minded governments.

Conclusion

If Congress believes that legislation is warranted, there are steps it can take to support the wider adoption of industry principles and ensure that U.S. companies are better equipped to respect human rights when operating in risky markets, such as:

- Encouraging companies to assess and better manage human rights risks associated with the provision of Internet products and services in repressive countries;
- Harnessing the knowledge and resources of the United States government to support better company decision-making when faced with challenges to free expression and privacy; and,
- Encouraging participation in relevant voluntary corporate social

[21] *See* CDT-BSR press release announcing multi-stakeholder principles initiative (Jan. 18, 2007): http://www.cdt.org/press/20070118press-humanrights.php.

responsibility initiatives.[22]

In sum, the challenges to global Internet freedom cannot be addressed by either government or industry alone. The U.S. government must leverage the powerful instruments of diplomacy, trade, and foreign aid in the service of Internet freedom, and companies must accept their obligations as human rights actors and exercise due diligence when facing free expression and privacy challenges in difficult markets. Collective action to develop industry principles is key as is greater collaboration between government and industry.

CDT looks forward to working with Congress on ways to advance global Internet freedom.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION

Please contact: Brock Meeks

Director of Communications

202-637-9800

[22] CDT is not convinced that proposals like Title II of the Global Online Freedom Act in the House [H.R. 275] (110th Congress), which place the U.S. government in an adversarial relationship with U.S. businesses, is either workable or wise. CDT recently wrote an analysis of GOFA (May 2, 2008): http://www.cdt.org/international/censorship/20080505gofa.pdf.