KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Written Submission of the **Center for Democracy & Technology**

Before the Senate Judiciary Committee,
Subcommittee on Human Rights and the Law

GLOBAL INTERNET FREEDOM AND THE RULE OF LAW II

March 2, 2010

Chairman Durbin, Ranking Member Coburn, and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to submit this written statement. We applaud the Subcommittee's leadership and continued attention to corporate responsibility and Internet freedom.

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. However, the challenges to global Internet freedom have only grown more complex and difficult since this Subcommittee's hearing in 2008 on the issue.[1] Authoritarian regimes are increasingly enlisting companies and the technologies they produce to remake the Internet into a tool of political control. Last year, China asked computer manufacturers to pre-install the Green Dam filtering software on all computers sold in China in an attempt to further decentralize its censorship regime.[2] Many governments are increasingly building up surveillance and censorship capabilities using technologies developed in the west.[3] And authoritarian regimes are becoming ever more sophisticated in using new media technologies to propagate their own messages and control online debate.[4]

Just as important, many of our democratic allies are taking actions in the name of addressing various social ills that also jeopardize the environment for expression and innovation on the Internet. An Italian court just convicted three Google employees for a video posted by a user under the theory that might force companies to review all user-

---

[1] For our previous testimony to this Committee on this issue, see *Global Internet Freedom: Corporate Responsibility and the Rule of Law: Hearing before the Senate Judiciary Comm. Subcomm. on Human Rights and the Law*, 110th Cong. (2008) (statement of Leslie Harris, President & CEO, Center for Democracy & Technology), http://www.cdt.org/testimony/testimony-leslie-harris-global-internet-freedom-corporate-responsibility-and-rule-law.

[2] OpenNet Initiative Bulletin, "China's Green Dam: The Implications of Government Control Encroaching on the Home PC," OpenNet Initiative, July 27, 2009, http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.

[3] See, e.g., Helmi Noman, "Middle East Censors Use Western Technologies to Block Viruses and Free Speech," OpenNet Initiative Blog, http://opennet.net/blog/2009/07/middle-east-censors-use-western-technologies-block-viruses-and-free-speech; Naomi Klein, "China's All-Seeing Eye," Rolling Stone, May 29, 2008, http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye/print.

[4] *Global Internet Freedom: Corporate Responsibility and the Rule of Law II: Hearing before the Senate Judiciary Comm. Subcomm. on Human Rights and the Law*, 111th Cong. (2010) (statement of Rebecca MacKinnon, Visiting Fellow, Princeton University), http://rconversation.blogs.com/files/rm_sjc_2march2010.pdf.

generated content before it can be hosted on their services in Italy.[5] In an overbroad claim of jurisdiction, Belgium authorities have ignored existing treaties and imposed fines on Yahoo! for refusing to hand over user data.[6] And Australia is advancing a mandatory Web filtering proposal that requires ISPs to implement a secret government blacklist for prohibited content (an approach that is of questionable efficacy in fighting child exploitation).[7] Authoritarian regimes often point to such actions by democratic governments to justify their own acts of censorship and surveillance.[8]

Advancing Global Internet Freedom Requires Action on Multiple Fronts

The Internet has developed and flourished because of a policy framework based on competition, openness, innovation, and trust. That framework puts power not in the hands of centralized gatekeepers but in users and innovators at the edges of the network. It protects intermediaries such as ISPs and Web hosts from liability for content created by their users. And this framework minimizes government interference. Under this approach, the Internet is able to fulfill its potential as an engine of democratization, economic growth and human development.

However, as the above examples illustrate, this policy framework is under threat globally and U.S. leadership and advocacy is urgently needed worldwide. Secretary of State Clinton's landmark speech in January 2010 elevated global Internet freedom high on the foreign policy agenda of the United States. Clinton's speech should be a starting point for a broad and sustained effort by the U.S. government to keep the Internet open, innovative and free. To implement the Secretary's vision, CDT urges the U.S. government to take action in four areas:

1. Guard Internet freedom at home
2. Advocate for Internet freedom through all the tools of diplomacy, trade, and foreign aid at the government's disposal
3. Support Internet activists all over the world
4. Promote and support corporate social responsibility in the ICT sector

Companies, Congress, and a wide range of U.S. governmental actors can play a key role in advancing efforts in all four areas.

---

[5] Thomas Claburn, "Google Execs Convicted in Italy," Information Week, February 24, 2010, http://www.informationweek.com/news/hardware/utility_ondemand/showArticle.jhtml?articleID=223100601. See also, Leslie Harris, "Deep Impact: Italy's Conviction of Google Execs Threatens Global Internet Freedom," Huffington Post, February 24, 2010, http://www.huffingtonpost.com/leslie-harris/deep-impact-italys-convic_b_474648.html.

[6] Cynthia Wong, "Yahoo! protects user privacy – and gets fined?", Policy Beta Blog, July 11, 2009, http://www.cdt.org/blogs/cynthia-wong/yahoo-protects-user-privacy-and-gets-fined.

[7] Andrew McDiarmid, "Filtering Down Under," Policy Beta Blog, December 18, 2009, http://www.cdt.org/blogs/andrew-mcdiarmid/filtering-down-under.

[8] See, e.g., Leslie Harris, "21st Century Statecraft: the Internet as Diplomat," Ahead of the Curve, ABC, http://abcnews.go.com/Technology/AheadoftheCurve/internet-diplomat-21st-century-statecraft/story?id=9740416&page=3 (quoting a translated reaction from a Chinese official to Secretary of State Clinton's speech on Internet freedom).

Companies are key actors in keeping the Internet open and free

Governments hold the primary obligation to protect human rights, and one ultimate goal of any collective strategy to advance Internet freedom must be to change the behavior of Internet-restricting countries themselves. However, as the UN Special Representative on business and human rights John Ruggie has determined, while "their responsibilities cannot and should not mirror the duties of States," companies have a responsibility to respect human rights.[9] Secretary of State Clinton confirmed this notion in her speech in January, saying, "[t]he private sector has a shared responsibility to help safeguard free expression. And when their business dealings threaten to undermine this freedom, they need to consider what's right, not simply what's a quick profit."[10]

Communications technologies and new media services have become vital to the lives of millions of users all over the world. We have seen extraordinary examples of the ability of these technologies to amplify voices and speak truth to power in Iran, Burma, and Tibet in the past two years. Just as important, these technologies offer new ways for citizens in all countries to come together, speak out on common concerns, and participate in their own governance. The products and services offered by even the smallest Internet start-up can be potentially reached by any user on the global Internet. But "[n]o matter where you live, people want to believe that what they put into the Internet is not going to be used against them."[11] Just as good corporate citizens strive to minimize the environmental impact of their operations and prevent labor violations in its workforce, ICT companies must address the risks to freedom of expression and privacy raised by their business operations.

Exercise due diligence and avoid complicity in human rights violations

First and foremost, companies have a responsibility to avoid complicity in governmental acts of censorship and surveillance. John Ruggie has set forth a thoughtful framework for corporate responsibility that centers on the exercise of "due diligence," which 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 proactive strategies to minimize human rights risk; and
- Ongoing monitoring and auditing to track performance and improve practices.[12]

As intermediaries between governments and citizens, technology companies will face increasing pressure from governments to implement Internet controls as a way of decentralizing state Internet repression. In addition, even if a company is merely offering

---

[9] John Ruggie, *Protect, Respect and Remedy: a Framework for Business and Human Rights*, at 16-17 (April 7, 2008), http://www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf.

[10] Secretary of State Hilary Rodham Clinton, Remarks on Internet Freedom, Newseum, Washington, DC, January 21, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm.

[11] Secretary of State Clinton, Remarks on Internet freedom, *supra* note 9.

[12] Ruggie report, *supra* note 8, at 17-19.

their product for sale, where technologies can be used for both good and bad, companies have a responsibility to mitigate the impact of foreseeable uses of their products by states that seek to transform ICTs into a tools of political control. Companies must exercise due diligence in anticipating and addressing these risks.

When governments enlist companies in acts of censorship and surveillance, companies have a range of options for how they respond, almost all of which will fall short of pulling out of a difficult market. Specific company decisions about what products and services to offer (and to what customers), how those products and services are designed, and how the company responds to government requests to take down user content or hand over user data can have an enormous impact on users' ability to speak and protect their privacy.

The Green Dam incident in 2009 and Google's announcement in January 2010 on its operations in China make clear that companies can no longer passively ignore the human rights risks that arise in the ICT sector or engage in unthinking adherence to local law:[13] The ethical dilemmas are only going to get harder, and companies must have a thoughtful, systematic, and proactive approach in how they will respond, or else risk complicity in human rights violations and the loss of user trust in their business practices and products.

Promote practices that guard Internet freedom

Companies also have a responsibility to promote policies and practices by governments – at home and abroad – that guard Internet freedom. Governments all over the world are struggling to address longstanding social ills in the new digital era. But when governments seek to surveil without a warrant in the name of security, impose filtering mandates to protect children, or threaten to cut Internet access for users to enforce intellectual property laws, companies must make the case that the adoption of such policies in democratic countries make all the more difficult for them to operate responsibly elsewhere in the world. No market is without ethical risk, and the ICT sector has a clear role to play in advocating for governmental policies and practices that protect user rights all over the world, including at home.

Collaborate with stakeholders

The Global Network Initiative (GNI) provides a framework for companies to systematically examine and mitigate the human rights risks their businesses face in various countries. After extensive consultation, research, and benchmarking, the GNI produced a set of high-level Principles and detailed Implementation Guidelines that begin to develop a standard for corporate responsibility and human rights due diligence in the ICT sector. These Principles and Guidelines provide operational guidance for ethical company decision-making all around the world. GNI companies commit to implementing the Principles throughout their operations, conducting human rights risk assessments, and crafting strategies to mitigate risks presented – all with the help and support of human rights and technology policy experts, investors, and academics. The

[13] Cynthia Wong, Deconstructing Green Dam, Policy Beta Blog, August 24, 2009, http://www.cdt.org/blogs/cynthia-wong/deconstructing-green-dam.

GNI also acts as a platform for collaboration on key issues of government policy and for collective action when emerging threats to Internet freedom arise. Companies strengthen their hand when they work with other companies and non-company stakeholders to push back against government demands that impact human rights.

Companies who join the GNI not only benefit from this framework for engagement and collaboration, but also more credibly demonstrate their commitment to addressing human rights risk by engaging in a transparent and accountable way.. To be clear, GNI's accountability mechanisms are not a "gotcha" exercise: The goal is to improve company processes and to enhance the Principles and Guidelines over time through a collaborative learning process,.

In CDT's view, GNI offers the most promising path forward for companies to join with other key stakeholders to address the challenge of Internet freedom. While it may be possible for a company to find an alternative means of managing human rights risk, it is it is demonstrably clear that doing nothing is no longer an option.

Congress should promote corporate responsibility and support companies in managing human rights risks

Ensure companies are exercising human rights due diligence

Congress can play an important role in ensuring companies are acting responsibly. Congress should encourage industry adoption of the UN Special Representative Ruggie framework for corporate responsibility and exercise of human rights due diligence. Policymakers can support companies in conducting human rights impact assessments (HRIAs) by assisting efforts to craft tools and standards for assessing human rights risk in the ICT industry and to develop strategies for mitigating risk. Because GNI members have done extensive benchmarking on ICT-focused risks, Congress should encourage companies to join the GNI and take advantage of the collective expertise and real-time problem solving assistance that the GNI offers.

Congress can also encourage greater information sharing between companies and relevant government agencies around human rights challenges the ICT industry faces and how the industry is responding. Such exchange could help better inform development of policy and diplomatic strategies, as well as serve as a resource for companies striving to minimize human rights risks in their business. However, such data sharing must be implemented in a way that protects personal user information and does not introduce additional confidentiality concerns.

Finally, if Congress acts legislatively, we urge Congress to do so in a way that both incentivizes *and* supports responsible engagement by companies across the ICT industry. While CDT supports the goals of the Global Online Freedom Act of 2009 (GOFA) [H.R. 2271], the approach this legislation takes may be impractical in implementation and under-inclusive at best, and may do more harm than good at worst.[14] GOFA does not address the roles and actions of a range of companies that

[14] For CDT's analysis of a previous iteration of the Global Online Freedom Act [H.R. 275, 110th], see CDT, "Analysis of the Global Online Freedom Act of 2008 [H.R. 275]: Legislative Strategies to Advance Internet Free Expression and Privacy Around the World," May 2, 2008, http://cdt.org/international/censorship/20080505gofa.pdf.

provide hardware, software, and telecommunications products. In addition, the specific mandates that GOFA would place on delivery of Internet services in Internet restricting countries may even discourage provision of these vital platforms for expression.

Address the export of technologies to countries with a demonstrated history of Internet repression

Many of the most Internet-restrictive regimes use technology developed by American companies to implement their systems of censorship and surveillance.[15] The companies at issue have had varying degrees of direct involvement in the sales, installation, consultation, and training associated with such governmental uses of their technologies.

Congress should direct an examination of whether narrowly targeted export restrictions are necessary for technology or related services that enable surveillance or censorship in countries with a demonstrated history of Internet repression (or where use of technologies or services to facilitate human rights violations is reasonably foreseeable). These restrictions should apply especially where technologies and services are specifically designed or customized to enable governmental censorship or surveillance in high-risk countries.

However, the U.S. government must also ensure our export policies do not chill free expression on the global Internet. Even some of the strictest sanctions provided by U.S. law carve out exceptions for information and information materials, or transactions involving books, journals, and newspapers.[16] The goal of these exceptions is to support free expression and access to information in countries where discourse and media are tightly controlled. However, many of these regulations were passed before the advent of new media tools and user generated content services such as instant messaging clients, social networking sites, and even web hosting services. In the face of uncertainty about how these rules apply to new technologies (and threat of fines if a company missteps), companies may hesitate to offer communications technologies and platforms for speech to sanctioned countries[17] – resulting in a policy misalignment that serves to undermine U.S. foreign policy goals around promoting human rights and democratic values.

We are encouraged by the Obama Administration's announcement this March to issue a general license for the export of many of these new media tools.[18] CDT encourages Congress and the Administration to further examine other changes necessary to promote the use of tools by advocates in sanctioned countries that expand free expression and access to information, while also protecting user privacy.

---

[15] See, e.g., Helmi Norman, "Middle East Censors Use Western Technologies to Block Viruses and Free Speech," OpenNet Initiative, July 27, 2009, http://opennet.net/blog/2009/07/middle-east-censors-use-western-technologies-block-viruses-and-free-speech; Rebecca MacKinnon, "More on Cisco in China," RConversation, June 30, 2005, http://rconversation.blogs.com/rconversation/2005/06/more_on_cisco_i.html.

[16] See, e.g., 31 C.F.R. § 560.210(c) and § 560.315 (exempting informational materials such as publications, films, posters, and news wire feeds from the Department of the Treasury, Office of Foreign Assets Control regulations on Iran).

[17] See Eric Lai, "Should Facebook, Twitter follow IM providers and block access to U.S. 'enemies'?", Computerworld, June 10, 2009, http://www.computerworld.com/s/article/9134233/Should_Facebook_Twitter_follow_IM_providers_and_block_access_to_U.S._enemies_.

[18] Mark Landler, "U.S. hopes Internet Exports will Help Open Closed Societies," New York Times, March 7, 2010, http://www.nytimes.com/2010/03/08/world/08export.html?ref=technology.

Support and equip companies to deal with government requests that violate human rights

While some argue that technology companies should simply withdraw from challenging markets, most Internet freedom advocates agree with CDT that the *responsible* engagement by the U.S. ICT industry in these markets – and the communications platforms, information services, software and hardware they provide – play an important role in expanding global Internet freedom. Many companies are struggling to find an ethical path forward, sometimes pushing back or finding ways to skirt the edges of vague censorship mandates, and other times stumbling badly and inadvertently facilitating human rights violations.[19] A broad range of governmental actors can help support and equip companies striving to be instruments of Internet freedom all over the world:[20]

- Support more extensive country reporting by the State Department on the legal, political, and policy environment for Internet freedom.
- Support training of officials and staff in the Department of State, Department of Commerce, the Office of the USTR, and other relevant agencies on global Internet freedom issues with the goal of enabling agency staff to aid companies and Internet advocates abroad, intervene where threats to Internet freedom arise, and integrate Internet freedom as a vital component of all American foreign policy.
- Encourage greater information sharing between government, industry, and NGOs about emerging human rights challenges. However, increased information sharing must be implemented in a way that protects user information and does not introduce new privacy concerns.

Provide technical support for Internet users and activists

As governments are becoming increasing sophisticated in controlling information and silencing political dissent online, Internet users and activists in closed societies need a range of training, technology and support to counter novel means of control and the Internet policies that enable such control.[21] Congress should:

- Fund dissemination of and training for a range of tools that enable circumvention of content controls and protect privacy across multiple platforms (web, wireless, mobile, etc.).
- Incentivize private sector development of technologies that enhance users' ability to circumvent content controls and protect their privacy.

---

[19] See, e.g., Erica Naone, "Search Engines' Chinese Self-Censorship," Ahead of the Curve, ABC, July 1, 2008, http://abcnews.go.com/Technology/AheadoftheCurve/story?id=5280133&page=1 and Nart Villeneuve, *Breaching Trust: An analysis of surveillance and security practices on China's TOM-Skype platform*, October 2008, http://www.nartv.org/2008/10/01/breaching-trust-tom-skype/.

[20] See also *Global Internet Freedom: Corporate Responsibility and the Rule of Law II: Hearing before the Senate Judiciary Comm. Subcomm. on Human Rights and the Law*, 111th Cong. (2010) (statement of Daniel J. Weitzner, Associate Administrator for Policy Analysis and Development, National Telecommunications and Information Administration, Department of Commerce).

[21] Testimony of Rebecca MacKinnon, *supra* note 4.

- Fund efforts to support NGOs engaged in policy reform efforts in countries around the world. Creating and preserving a policy framework that supports openness and trust on communications networks is a vital underpinning to all Internet freedom efforts. Advocates need to build capacity to promote sound Internet policies, in addition to protesting censorship.

Ensure domestic policies set the right example abroad

Finally, Internet freedom begins at home and the U.S. must lead by example. The U.S. is facing a range of complex policy challenges, from cybersecurity to intellectual property to protecting children online. The policy solutions we adopt must also take Internet freedom goals into account, and these solutions should be crafted in an open and accountable way, subject to public debate. Finally, we must take care not to set precedents that can be used by authoritarian regimes to justify their own acts of censorship and surveillance.

In sum, the ICT industry and a range of U.S. governmental actors have vital roles to play to advance global Internet freedom and ensure communications technologies remain engines of democratization, economic growth, and human development. CDT applauds Senator Durbin, Senator Coburn, and the other members of the Subcommittee for their continued commitment to this issue. CDT looks forward to working with Congress on ways to keep the Internet open, innovative, and free.

##

For more information, please contact:

Leslie Harris, President & CEO
lharris@cdt.org
(202) 637-9800 x115

Cynthia Wong, Ron Plesser Fellow
cynthia@cdt.org
(202) 637-9800 x117