

May 2, 2008

**ANALYSIS OF THE  
GLOBAL ONLINE FREEDOM ACT OF 2008 [H.R. 275]:  
*Legislative Strategies to Advance Internet Free Expression and Privacy Around the World***

**I. INTRODUCTION**

On January 5, 2007, Rep. Chris Smith (R-NJ) and Rep. Frank Wolf (R-VA) introduced the Global Online Freedom Act [H.R. 275] (“GOFA”).<sup>1</sup> The goal of the bill is to use United States influence – both governmental and commercial – to advance Internet freedom in repressive regimes.

More specifically, the bill encourages the President to make the promotion of free expression and privacy on the Internet a top foreign policy priority of the United States; creates an Office of Global Internet Freedom at the State Department that is responsible for coordinating Internet freedom efforts and conducting research; and mandates that U.S. Internet companies take certain actions to combat censorship and protect personal information, or otherwise be subject to criminal or civil prosecution by the U.S. attorney general or civil lawsuits brought by private litigants.

The Center for Democracy & Technology (CDT) strongly supports the goals of the Global Online Freedom Act. CDT’s core mission is to advocate for a global Internet that is open, innovative and free. Countries around the world are increasingly resorting to censorship and surveillance on the Internet.<sup>2</sup> We believe the United States government should make the promotion of Internet freedom a top foreign policy priority.

We also believe that companies have a responsibility to take actions that protect the free

---

<sup>1</sup> On December 10, 2007, H.R. 275 was amended and reported favorably by the House Foreign Affairs Committee. This analysis is based on an Amendment in the Nature of a Substitute dated February 21, 2008 (12:19 p.m.).

<sup>2</sup> For a comprehensive examination of Internet filtering and surveillance, see the reports of the OpenNet Initiative, <http://opennet.net/>.

expression and privacy rights of their users. To that end, CDT has been co-facilitating a multi-stakeholder dialogue among Internet and telecommunications companies, human rights groups and other civil society organizations, investors and academics to draft a set of voluntary global principles to guide the technology industry in the protection of privacy and free expression around the world.

CDT is concerned, however, about specific mandates that GOFA would place on the delivery of services in Internet-restricting countries, and we question whether those mandates might do more harm than good. Below we analyze key sections of the bill, highlighting both those provisions that we support and those that we believe raise concerns.

## **II. ANALYSIS OF GLOBAL ONLINE FREEDOM ACT OF 2008 [H.R. 275]**

### **TITLE I: Promotion of Global Internet Freedom**

#### **Section 101. Statement of Policy**

CDT strongly supports this statement of U.S. policy, and in particular the declaration that the U.S. shall “use all appropriate instruments of United States influence, including diplomacy, trade policy, and export controls” to promote global Internet freedom.<sup>3</sup>

We are less clear that it makes sense to position U.S. companies and their government as adversaries on global Internet freedom as Sec.101(3) suggests. If the ultimate goal is to change the behavior of Internet-restricting countries in effecting the political censorship of online content”, the U.S. government must work collaboratively with U.S. companies to help them navigate these difficult legal environments and to put pressure on these regimes to change their censorship laws.

#### **Section 102. Sense of Congress**

Sec. 102(2) states that US businesses that collaborate with IRCs to block VOA-type content are working against US foreign policy interests and tax-payer funded efforts to promote free expression. Compliance with local law and fealty to US policies is often not possible in many contexts. Congress’s goal here must be to help equip U.S. businesses to better respond to these challenges.

#### **Section 103. Annual Country Reports on Human Rights Practices**

CDT strongly supports Section 103, which requires the State Department to include analyses related to Internet freedom in its annual Country Reports on Human Rights Practices.<sup>4</sup>

---

<sup>3</sup> GOFA § 101(2).

<sup>4</sup> <http://www.state.gov/g/drl/rls/hrrpt/>.

We urge that the information collected on Internet access and use in a country, government attempts to censor content and access personal information, and government prosecutions of cyber-dissidents also be used to inform the U.S. government's decision-making related to the granting of foreign aid and the development of trade agreements,<sup>5</sup> and to provide guidance to companies seeking to do business in Internet-restricting countries.

#### **Section 104. Office of Global Internet Freedom**

CDT strongly supports 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.<sup>6</sup>

CDT also supports in principle the multi-stakeholder approach outlined in Section 104(b)(6), which requires, in part, the Office of Global Internet Freedom to “establish a regularized consultative process with appropriate technology companies involved in providing, maintaining or servicing the Internet, human rights organizations, academic experts, and others to develop a voluntary code of minimum corporate standards related to Internet freedom.” We note, however, that a similar effort has been underway since late 2006 – with the encouragement but not the participation of the State Department – and is drawing to a conclusion. We see no reason to duplicate this effort in a new statutorily mandated initiative and suggest that the Office be tasked with activities that will build upon the current effort and encourage broad industry adoption of the resulting voluntary principles.

#### **Section 105. Annual Designation of Internet-Restricting Countries; Report**

CDT generally supports Section 105, which requires the State Department to make a list of “Internet-restricting countries” based on evidence that “the government of the country is directly or indirectly responsible for a systematic pattern of substantial restrictions on Internet freedom during any part of the preceding 1-year period.” However, to ensure credibility, it is critical that the process of designation be even-handed and untainted by other foreign policy considerations.<sup>7</sup>

### **TITLE II: Minimum Corporate Standards for Online Freedom**

#### **Section 201. Protection of Personally Identifiable Information**

Section 201 applies to three kinds of U.S. businesses: Internet search engines, Internet content hosting providers, and companies that offer Internet communications services. These

---

<sup>5</sup> The European Union has taken steps to treat Internet censorship as a trade barrier, <http://arstechnica.com/news.ars/post/20080227-eu-may-begin-treating-net-censorship-as-a-trade-barrier.html>.

<sup>6</sup> We assume that the activities of the Global Internet Freedom Task Force (GIFT) launched by the State Department in 2006 would be subsumed by this new office, <http://www.state.gov/g/drl/rls/78340.htm>.

<sup>7</sup> For example, information compiled by the OpenNet Initiative makes the case that some key United States allies engage in Internet-restricting practices that are “systematic” and “substantial.” See GOFA § 105(a)(2).

companies may not “locate” within an Internet-restricting country 1) “any electronic communication” 2) that contains “personally identifiable information used to establish or maintain an account for Internet communications services” 3) where such services enable “political, religious, or ideological opinion or belief” to be expressed.

We are sympathetic to the goal of this provision, which is to place personal information beyond the reach of Internet-restricting governments, but we are highly skeptical of the wisdom or efficacy of such an approach. We agree that companies doing business in difficult legal environments need to take account of the risks to human rights in designing their services and take steps to minimize those risks. How a company handles customers’ personal information in such an environment is a key risk management question. Minimization of data collection and limited data retention, in addition to off-shore location of servers may be appropriate strategies in some circumstances.

However, a mandate to keep customers’ personal data out of the country *in all cases* is unworkable and unlikely to provide the protection envisioned by the legislation. Our concerns about the proposal include:

First, where data is stored is often irrelevant to countries’ assertion of jurisdiction over Internet-based content or service providers. Many countries assert jurisdiction over a company (and thus the information it maintains, even that information is stored off-shore) if that company simply does business in a country or if the company’s content or services merely reach the country’s citizens on the global Internet, even if the company was not actively trying to target that market.<sup>8</sup> Moreover, the presence of employees who may be subject to imprisonment and assets that may be subject to forfeiture usually make it extremely difficult to resist a claim of jurisdiction.

Second, we fear that any mandate to U.S. companies to store data outside of Internet restricting countries will simply provoke those countries to retaliate by requiring companies to store personal information about local users on servers located within their borders, thereby placing the companies in the untenable situation of having to comply with conflicting laws of the U.S. and such host countries.

Third, some services out of necessity require the storing of personal information inside the country where they are being used. For example, the Internet phone service (VoIP) Skype relies on a peer-to-peer network that enables customers to make their phone calls by connecting via other local Skype customers’ computers. The service works by storing on users’ local computers identifying information about other users needed to establish connections between users of the Skype network. The same is true for other services that rely on a peer-to-peer architecture and allow users to find each other or address communications using personally identifiable information (e.g., name or email address).

Fourth and finally, the quality and speed of some Internet services may be degraded if

---

<sup>8</sup> See, e.g., *Gutnick v Dow Jones & Co Inc* [2001] VSC 305 (28 August 2001), <http://www.austlii.edu.au/au/cases/vic/VSC/2001/305.html>.

required to be partially managed on hardware located outside the target market. For example, some services that involve real-time communication, such as video conferencing and instant messaging (IM), may require continual or occasional authentication or exchange of user information with a central server during the course of a video conference or IM session. If the central server is located outside the country where the services are being offered, the time it takes to exchange information with the server will increase, potentially degrading the quality of the communication.<sup>9</sup>

## **Section 202. Integrity of Personally Identifiable Information**

Unlike Section 201, Section 202(a) is not limited to Internet companies. Any U.S. company that “collects or obtains personally identifiable information through the provision of products or services on the Internet” is required to provide the PII to a “foreign official of an Internet-restricting country” *only for* “legitimate foreign law enforcement purposes as determined by the Department of Justice.”<sup>10</sup> We understand that the goal of this provision is to limit the possibility that a United States company’s local subsidiary will turn over information to an Internet-restricting country that would be used to punish cyber-dissidents or otherwise violate human rights.

While we believe that the United States government should provide any guidance it can to companies to help them navigate the uncertain legal terrain presented in many of the countries at issue here, we are less certain how Section 202(b) would work in practice, which would require U.S. companies only to use “established legal channels as approved by the Attorney General as secure and otherwise appropriate” when disclosing customers’ PII to officials of Internet-restricting countries for “legitimate foreign law enforcement purposes.” It is unclear whether the section is intended to require U.S. companies to seek case-by-case approval from the Department of Justice or whether DOJ is expected to designate in advance “legitimate foreign law enforcement purposes” and “established legal channels” for each Internet-restricting country. In any case, either approach may not prevent Internet-restricting countries from shaping illegitimate demands for PII in a manner that conforms to DOJ rules.

We strongly favor more robust company resistance and challenge to demands for information where human rights may be at risk and we would encourage greater collaboration between companies and the United States government to identify and respond to high-risk cases. We are concerned, however, with a legal mandate (indeed a mandate backed up by criminal penalties) that may require companies to defy local law would either risk civil or criminal

---

<sup>9</sup> Even if the off-shore location mandate were workable, Section 201 does not protect a significant amount of sensitive personal information. If we read the various definitions correctly, personal information in the *content* of an electronic mail is not protected, nor is personal information stored *statically* (because Section 201 only addresses personal *account* information in an *electronic communication*, which is a *transfer* of data).

<sup>10</sup> We do not understand the rationale for limiting application of Section 201 to “Internet companies” and yet applying Section 202 to all U.S. businesses. If the goal of these sections is to shield personal information from the reach of a repressive regime, then the same rules ought to apply to all companies that collect relevant PII. Credit card transactions, for example, can reveal memberships in forbidden groups, purchases of books, travel and other activities that can be used to build a case against a political dissident. Yet, that data may be stored in an “Internet restricting country” under this bill.

sanction of local employees or to force U.S. companies to abandon some markets. On balance, we do not believe that the withdrawal of U.S. companies from Internet-restricting countries would serve the aims of Internet freedom.

### **Section 203. Transparency Regarding Search Engine Filtering**

Section 203 would require search engines to provide the Office of Global Internet Freedom “all terms and parameters used to filter, limit, or otherwise affect the results provided by the search engine that are implemented: (1) at the request of, or by reason of any other direct or indirect communication by, any foreign official of an Internet-restricting country; or (2) to comply with a policy or practice of restrictions on Internet freedom in an Internet-restricting country.”

CDT supports this provision insofar as the information collected informs the U.S. government’s understanding of the practices of Internet repressive countries and guides the development of country-specific diplomatic strategies. We are not persuaded, however, that *public reporting* of such activities, except perhaps in aggregate form, would further the aims of the bill. While Internet companies should inform their users that content has been removed pursuant to the law of Internet-restricting countries, public disclosure of company-by-company practices may be counterproductive. Disclosure may increase pressure on the companies to do better, but it may also lead Internet-restricting countries to demand more rigorous adherence to the laws, particularly since the local subsidiaries of U.S. companies are likely to interpret vague mandates to censor less zealously than their domestic counterparts

### **Section 204. Transparency Regarding Internet Censorship**

We have similar concerns with Section 204’s mandate that Internet content hosting companies provide the Office of Global Internet Freedom with the URLs of all websites that have been removed or blocked pursuant to government requests, policies and practices. We support the collection of information to inform government activities, including providing guidance, advice and support to companies. However, we question the impact of public disclosure. We also note that there are many laws globally that require removal of content that may not implicate Internet freedom such as those dealing with child pornography and intellectual property; in many cases these laws also prohibit disclosure of the URL list used to block or remove access to content. <sup>11</sup>

## **TITLE III: Export Controls for Internet-Restricting Countries**

CDT believes that it is appropriate to investigate whether some technologies that may be used for surveillance and suppression of speech should be subject to export controls. Therefore, we support conducting the “feasibility study regarding the development of export controls”

---

<sup>11</sup> We also note that many democratic ones forbid disclosure of URLs or terms that are required to be blocked with respect to child pornography. See, <http://www.fsm.de/en/CoC> (describing German practices); [http://www.acma.gov.au/WEB/STANDARD/pc=PC\\_90080](http://www.acma.gov.au/WEB/STANDARD/pc=PC_90080) (Australia); <http://www.cybertip.ca/app/en/cleanfeed> (Canada). And of course repressive countries like China often invoke state secrets laws, which make the disclosures required by the bill illegal.

outlined in Section 301.<sup>12</sup>

### III. CONCLUSION

CDT shares Congress' commitment to global Internet freedom. We strongly believe that the promotion of Internet freedom should be fully integrated into all aspects of foreign policy, trade and financial aid, and thus we generally support Title I. We also agree that United States companies have a responsibility to respect human rights and to engage, when operating in difficult markets, in rigorous risk assessments designed to limit the risk of harm to their users.<sup>13</sup> However, we believe that some of the mandates in Title II are unworkable and unlikely to protect rights, might even be counterproductive, and are likely to limit the ability of U.S. companies to provide Internet-related services in Internet-restricting countries, which we believe, on balance, helps to advance Internet freedom and democratic values.

That said, we believe that Congress has a role to play in promoting global Internet freedom:

- First, by taking actions that encourage companies to assess and better manage human rights risks associated with the provision of services in Internet-restricting countries;
- Second, by harnessing the resources of the United States government to support better company decision-making when faced with challenges to free expression and privacy; and
- Third, by encouraging participation in relevant corporate social responsibility initiatives.

CDT looks forward to working with Congress on the important issue of global Internet freedom.

###

---

<sup>12</sup> Keith Bradsher, "At Trade Show, China's Police Shop for the West's Latest," *New York Times* (April 26, 2008), <http://www.nytimes.com/2008/04/26/business/worldbusiness/26security.html>.

<sup>13</sup> The recent report of the United Special Representative on Human Rights and Transnational Corporations, John Ruggie, offers a helpful framework for Congress to consider the responsibilities of companies with respect to human rights. See "Protect, Respect and Remedy: A Framework for Business and Human Rights" (April 7, 2008), <http://www.business-humanrights.org/Links/Repository/965591>.