Boston College International and Comparative Law Review

Volume 30 | Issue 2 Article 8

5-1-2007

Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World

Christopher Stevenson

BREACHING THE GREAT FIREWALL: CHINA'S INTERNET CENSORSHIP AND THE QUEST FOR FREEDOM OF EXPRESSION IN A CONNECTED WORLD

Christopher Stevenson*

Abstract: In the final days of 2005, Microsoft Corporation made international headlines when it removed the site of a Beijing researcher from its blog hosting service. Soon, other instances of U.S. companies assisting in China's internet censorship emerged. These revelations generated outrage among commentators and legislators and led to calls for action. This Note examines the methods of internet censorship employed by China and other nations, and explores the assistance that U.S. companies have provided to these nations. It analyzes the liability issues facing these companies in light of existing case law and statutory solutions proposed in the U.S. Congress. It then proposes a novel combination of existing legislative proposals, recommendations from the Electronic Frontier Foundation, and international cooperation as the best way to address the problem of internet censorship.

Introduction

During the final days of December 2005, Microsoft Corporation, a U.S. company, removed the site of Beijing blogger Zhao Jing from its MSN Spaces service.[1] The move might have gone unnoticed by major media sources but for the fact that Zhao was a research assistant in the Beijing bureau of the New York Times.[2] Instead of fading away, the story broke in the U.S. media in January of 2006.[3]

---

* Christopher Stevenson is a Managing Editor of the *Boston College International & Comparative Law Review.*

[1] David Barboza & Tom Zeller Jr., *Microsoft Shuts Blog's Site After Complaints in Beijing,* N.Y. Times, Jan. 6, 2006, at C3; Andrew Donoghue, *Microsoft Censors Chinese Blogger,* CNET News.com, Jan. 4, 2006, http://news.com.com/Microsoft+censors+Chinese+blogger/2100–1028_3–6017540.html.

[2] Barboza & Zeller, *supra* note 1.

[3] *See* Barboza & Zeller, *supra* note 1; Editorial, *Beijing's New Enforcer: Microsoft,* N.Y. Times, Jan. 17, 2006, at A18.

Other instances of U.S. companies assisting China's censorship efforts soon made headlines.[4] The story of Shi Tao, a Chinese citizen sentenced to a ten year prison term for e-mailing a "state secret," caused a great deal of outrage when it was discovered that Yahoo! had provided the Chinese government with information linking the e-mail to the IP address of Shi's computer.[5] In the midst of this turmoil, Internet giant Google announced that it was starting Google.cn, a new search engine service hosted in China.[6] This new search engine would not include the blogging or e-mail capabilities of Google.com and would comply with Chinese government restrictions that censor any material deemed illegal or inappropriate.[7]

Appalled by what they saw as blatant violations of human rights, members of the U.S. Congress convened hearings in Washington D.C. on February 15, 2006.[8] Present were representatives from Microsoft, Cisco Systems, Google, and Yahoo!, as well as spokespersons from international watchdog and human rights groups such as Reporters Without Borders and Radio Free Asia.[9] Lawmakers lambasted the U.S. based Internet companies for their cooperation with the repressive Chinese censorship regime.[10] Representative Tom Lantos (D)-CA asked the representatives how their corporate executives could sleep at night and Representative Christopher Smith (R)-NJ compared the companies' activities to those of businesses that worked with the Nazi regime during World War II.[11] The following day, Representative Smith introduced

---

[4] *See* Sumner Lemon, *Yahoo May Have Helped Jail Another Chinese User,* NetworkWorld, Feb. 9, 2006, http://www.networkworld.com/news/2006/020906-yahoo-jail-user.html.

[5] Jim Kerstetter, *Group Says Yahoo Helped Jail Chinese Journalist,* CNET News.com, Sept. 6, 2005, http://news.com.com/Group+says+Yahoo+helped+jail+Chinese+journalist/2100–1028_3–5851705.html?tag=nl. The "state secret" Shi transmitted was the government's reporting guidelines surrounding the 15th anniversary of Tiananmen Square protests. *Id.*

[6] David Barboza, *Version of Google in China Won't Offer E-mail or Blogs,* N.Y. Times, Jan. 25, 2006, at C3.

[7] *Id.*

[8] Tom Zeller, Jr., *Web Firms Questioned on Dealings in China,* N.Y. Times, Feb. 16, 2006, at C1.

[9] Ctr. for Democracy and Tech.—Censorship, http://www.cdt.org/international/censorship/ (last visited May 5, 2007) (containing statements of these hearing participants).

[10] Declan McCullagh, *Politicians Lash out at Tech Firms over China,* CNET News.com, Feb. 16, 2006, http://news.com.com/Politicians+lash+out+at+tech+firms+over+China/2100–1028_3–6039834.html; Zeller, Jr., *supra* note 8.

[11] *The Internet in China: A Tool for Freedom or Suppression?: Joint Hearing Before the House Committee on International Relations,* 109th Cong. 5–7 (2006) (statement of Rep. Smith, Chairman, House Subcommittee on Africa, Global Human Rights and International Operations), *available at* http://www.foreignaffairs.house.gov/archives/109/26075.pdf; Zeller, Jr. *supra* note 8.

the "Global Online Freedom Act of 2006" that will, if passed, proscribe most of the censorship being conducted by companies such as Google.[12]

These hearings, and the outrage expressed by legislators, reporters, and Internet experts are only the latest salvos in the battle for online freedom of expression.[13] Legislators, scholars, and the Internet community have struggled for years to find a solution to the problem of governmental Internet restrictions in China and other countries and the apparent aid that U.S. companies have provided in the enforcement of those restrictions.[14] If the Internet is to remain a safe forum for the free and open exchange of ideas, lawmakers and the Internet community must work together to prevent repressive censorship.

Part I of this Note begins by exploring the history of Internet censorship laws. It then focuses on China's laws and its intricate system of information restriction known as "The Great Firewall of China." Finally, it examines the role U.S. companies have played in supporting these censorship regimes. Part II addresses the legal uncertainty surrounding the liability of U.S. companies that violate the laws of foreign countries and discusses two pieces of legislation, the Global Information Freedom Act and the new Global Online Freedom Act, which Congress has proposed as possible solutions to the problem. Part III examines the shortcomings of the Global Online Freedom Act and discusses how a combination of aspects of the Global Information Freedom Act, suggestions from the Electronic Frontier Foundation, and increased global cooperation is the best way to address this problem.

I. Background

For much of the 1990s, the Internet was seen as a great advance in promoting freedom of expression throughout the world.[15] It was assumed that the free flow of information would lead to freer socie-

---

[12] Tom Zeller Jr., *Internet Firms Facing Questions About Censoring Online Searches in China*, N.Y. Times, Feb. 15, 2006, at C3.

[13] *See* H.R. 4741, 109th Cong. (2006); H.R. 2216, 109th Cong. (2005); H.R. 48, 108th Cong. (2003) (attempting to enact the Global Internet Freedom Act in previous years).

[14] *See* Jim Hu, *Rights Group Looks at China and Techs*, CNET News.com, Nov. 27, 2002, http://news.com.com/Rights+group+looks+at+China+and+techs/2100–1023_3–975517. html; Rebecca MacKinnon, *China's Internet: Let a Thousand Filters Bloom*, YaleGlobal Online, June 28, 2005, http://yaleglobal.yale.edu/display.article?id=5928.

[15] Jack Goldsmith & Timothy Wu, *Digital Borders: National Boundaries Have Survived in the Virtual World—and Allowed National Laws to Exert Control over the Internet*, Legal Aff. Jan.-Feb. 2006, at 40; David Lee, *Multinationals Making a Mint from China's Great Firewall*, S. China Morning Post, Oct. 2, 2002, at 16, available at 2002 WLNR 4489164.

ties.[16] Unfortunately, the Internet has not been a liberating force as expected.[17] Governments that wish to restrict their citizens' access to certain information have proven remarkably adept at being able to do so—often with the help of U.S. companies.[18] To understand fully China's rationale for restricting information and the elaborate ends to which it and other countries will go to enforce their restrictions, it is useful to begin with a look at the laws and methods they employ.

A. *A Brief History of Internet Censorship*

China is by no means the only country censoring Internet content.[19] Many forms of restriction exist in many countries.[20]

1. Censorship by Laws

Some countries have employed their restrictions simply through laws preventing the display of materials deemed inappropriate. One of the earliest attempts at instituting this kind of censorship regime came, interestingly enough, from the United States.[21] In addition to prohibiting the transmission of obscene material and child pornography, the "Communications Decency Act of 1996" (CDA) attempted to criminalize the communication of "indecent" and "patently offensive" content to any person under 18 years of age.[22] The "patently offensive" and "indecent" material restrictions were immediately challenged and eventually struck down by the United States Supreme Court as overly vague and broad restrictions on freedom of speech.[23]

Congress tried again in 1998 by enacting the "Child Online Protection Act" (COPA).[24] This law had the same effect but was more narrowly tailored than the CDA and was not found to be unconstitutional

---

[16] Lee, *supra* note 15.

[17] *See* Goldsmith & Wu, *supra* note 15, at 41; Lee *supra* note 15.

[18] *See* Shanthi Kalathil & Taylor C. Boas, Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule 107–15 (2003); Elaine M. Chen, *Global Internet Freedom: Can Censorship and Freedom Coexist?*, 13 DePaul-LCA J. Art & Ent. L. 229, 246–48 (2003); MacKinnon, *supra* note 14.

[19] *See, e.g.,* Kalathil & Taylor, *supra* note 18, at 107–15 (detailing restrictions in China, Cuba, Singapore, Vietnam, Burma, the United Arab Emirates, Saudi Arabia, and Egypt).

[20] *See id.*

[21] *See* Reno v. Am. Civil Liberties Union (ACLU), 521 U.S. 844, 859–61 (1997) (evaluating 47 U.S.C. § 223).

[22] 47 U.S.C. § 223.

[23] *Reno v. ACLU,* 521 U.S. at 849.

[24] 47 U.S.C. § 231 (1998).

on its face.[25] Applying strict scrutiny, however, the Court ruled that the government still had the burden of proving that the restrictions in COPA were no more restrictive than necessary to advance the stated goal of protecting children from harm.[26] The government is still collecting data in an attempt to show that personal web filters—the Court's suggested alternative to COPA—are not as effective as COPA's provisions.[27]

A similar law has met with far more success in Australia.[28] The "Broadcasting Services Amendment (Online Services) Act" was passed in 1999 and regulates Internet content based on classifications made by a Classification Review Board: R18 (information deemed likely to be disturbing or harmful to persons under 18 years of age), X18 (nonviolent sexually explicit material involving consenting adults), and RC (refused classification).[29] Material in the X18 and RC categories is prohibited content regardless of whether or not it is only available to adults.[30] Material classified as R18 is allowed, but only on sites that restrict minors' access via a government approved adult verification system.[31]

Instead of searching for prohibited content, the government relies on public complaints to the Australian Communications and Media Authority (ACMA) to identify prohibited or potentially prohibited content.[32] When prohibited or potentially prohibited material is discovered on Australian servers, the ACMA issues take-down notices to Internet Service Providers (ISPs) and Internet Content Hosts.[33] When the prohibited content is hosted outside the country, the ACMA simply notifies approved makers of filtering and blocking software to add the content to their blacklists.[34]

---

[25] Ashcroft v. Am. Civil Liberties Union (ACLU), 535 U.S. 564, 566 (2002).

[26] Ashcroft v. Am. Civil Liberties Union (ACLU), 542 U.S. 656, 666 (2004).

[27] Arshad Mohammed, *Google Refuses Demand for Search Information,* WASH. POST, Jan. 20, 2006, at A1.

[28] Broadcasting Services Amendment (Online Services) Act, 1999, sched. 5, pt. 1 (Austl.), *available at* http://www.aph.gov.au/parlinfo/billsnet/99077.pdf [hereinafter Australian BSA].

[29] *Id.*

[30] ELECTRONIC FRONTIERS AUSTRALIA, INTERNET CENSORSHIP LAWS IN AUSTRALIA, http://www.efa.org.au/Issues/Censor/cens1.html (last updated Mar. 31, 2006) [hereinafter CENSORSHIP LAWS IN AUSTRALIA].

[31] *Id.*

[32] Australian BSA, *supra* note 28, at sched. 5 pt. 4. The ACMA does, however, have the authority to initiate investigations on its own. *Id.*

[33] CENSORSHIP LAWS IN AUSTRALIA, *supra* note 30.

[34] *Id.*

2. Censorship by Active Filtering

In contrast to the reactive systems used in Australia and proposed in the United States, the Internet censorship systems employed by many other countries rely on much more proactive filtering of Internet content.[35] Saudi Arabia is a good example of such a country.[36] In fact, it did not even allow public access to the Internet until it had established sufficient filtering technology in 1999.[37] The country is unusually open about its filtering mechanisms and policies.[38] The Internet Services Unit (ISU), which controls Internet access, maintains information about the filtering policy and mechanisms on its website.[39] The current prohibited content is described by a 2001 resolution of the Council of Ministers.[40] The ISU also maintains records of which users are online and which sites they access.[41]

In practice, the Saudi system seems focused on particular areas of government and religious concern.[42] Testing by the OpenNet Initiative revealed extensive Saudi filtering of sites dealing with pornography, drugs, gambling, and religious conversion.[43] Sites containing tools to circumvent filtering technologies are also blocked.[44] In contrast, sites dealing with homosexuality, religion, and even alcohol are relatively accessible.[45]

Other countries have introduced their own filtering systems.[46] Iran and Burma are notable for their extremely strict systems.[47] China

---

[35] Electronic Frontiers Australia, Internet Censorship: Law & Policy Around the World, http://www.efa.org.au/Issues/Censor/cens3.html (last updated Mar. 28, 2002).

[36] OpenNet Initiative, Internet Filtering in Saudi Arabia in 2004, http://www.opennetinitiative.net/studies/saudi/ [hereinafter Internet Filtering in Saudi Arabia].

[37] *Id.*

[38] *Id.*

[39] Internet Services Unit, Local Content Services Policy, http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring-policy.htm (last visited May 5, 2007); Internet Services Unit, Local Content Filtering Procedure, http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring-mechanism.htm (last visited May 5, 2007).

[40] Council of Ministers Resolution, Feb. 12, 2001, *available at* http://www.al-bab.com/media/docs/saudi.htm (banning access to any sites contrary to the state or its system, sites containing damaging news about the Kingdom or heads of state, sites containing subversive ideas, or sites infringing the sanctity of Islam or breaching public decency).

[41] *Id.*

[42] Internet Filtering in Saudi Arabia, *supra* note 36.

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *See* Censorship Laws in Australia, *supra* note 30.

[47] *See* OpenNet Initiative, Internet Filtering in Burma in 2005, Oct. 2005, *available at* http://www.opennetinitiative.net/burma/ONI_Burma_Country_Study.pdf; Open-

is clearly not the only offender in the Internet world, but it is the most sophisticated and effective.[48]

B. *China's Great Firewall*

The term "Great Firewall of China" is somewhat of a misnomer. Rather than using a single web filtering mechanism, China employees a complex system of laws, technology, and human oversight that effectively controls the web content available to users within China.[49] In the 1990s, few people would have believed this kind of control possible.[50] Many scholars believed that the world-wide expansion of the Internet would lead to the demise of repressive regimes as people around the world gained access to new ideas and information.[51] China was also worried about the impact of the Internet and structured its system accordingly.[52]

1. Legal Restrictions

Chinese Internet regulations on providers of Internet services are promulgated and enforced by a number of overlapping agencies.[53] The first major law to regulate Internet content was the 1996 "Interim Provisions Governing Management of Computer Information Networks in the People's Republic of China Connecting to the International Network."[54] The provisions were amended and enhanced in 1998 and 2000 by the "Provisions for the Implementation of the Interim Provisions Governing Management of Computer Information Networks in the People's Republic of China," State Council Order No. 292, "Measures on Internet Information Services" (IIS Measures), and the "Decision of

---

NET INITIATIVE, INTERNET FILTERING IN IRAN IN 2004–2005, *available at* http://www.opennetinitiative.net/studies/iran/ONI_Country_Study_Iran.pdf [hereinafter INTERNET FILTERING IN IRAN].

[48] *See* OPENNET INITIATIVE, INTERNET FILTERING IN CHINA IN 2004–2005, Apr. 14, 2005, *available at* http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf [hereinafter INTERNET FILTERING IN CHINA]; Derek Bambauer, *Cool Tools for Tyrants; The Latest American Technology Helps the Chinese Government and Other Repressive Regimes Clamp Down,* LEGAL AFF., Jan.-Feb. 2006, at 56.

[49] INTERNET FILTERING IN CHINA, *supra* note 48, at 3.

[50] *See* Goldsmith & Wu, *supra* note 15, at 40; Lee, *supra* note 15.

[51] *See* KALATHIL & BOAS, *supra* note 18, at 1–2, 14; Goldsmith & Wu, *supra* note 15, at 40; Lee, *supra* note 15.

[52] *See* Hu, *supra* note 14.

[53] *See* INTERNET FILTERING IN CHINA, *supra* note 48, at 8, app. 2.

[54] See Jill R. Newbold, *Aiding the Enemy: Imposing Liability on U.S. Corporations for Selling China Internet Tools to Restrict Human Rights,* 2003 U. ILL. J. L. TECH & POL'Y 503, 507–08.

the Standing Committee of the National People's Congress on Preserving Computer Network Security."[55] Taken as a whole, these regulations prevent Internet users and ISPs from displaying any content not approved by the government.[56] This includes content that divulges state secrets, subverts the government, opposes the State's policy on religion, advocates cults or feudal superstitions, disrupts the social order, or shows obscenity, pornography, gambling, or violence.[57]

All Internet information services must be licensed (if commercial) or registered with the authorities (if private).[58] If they provide news, publishing, bulletin board, or "other services," site operators must record the IP address and domain name information of all content provided.[59] ISPs must record and retain for sixty days the amount of time users spend online, their account numbers, their IP addresses, and their dial-up numbers.[60] If the site operator or ISP discovers prohibited information, it must be removed immediately, and records of the event must be retained and communicated to the appropriate authorities.[61]

The latest addition to this string of regulations came in 2005 and deals specifically with providers of "Internet news information services."[62] The term "Internet news" is defined broadly as "information on current and political affairs, which includes reports and comments on social public affairs such as those relating to politics, economy, military and diplomatic affairs and sudden events of society"[63] The regulation applies to anyone who publishes news information on websites, provides bulletin board system services on current and political topics, or transmits information on current and political topics to the public.[64] The new law contains all of the content restrictions and information retention of earlier laws, but adds the requirement that any

---

[55] *See* Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security, Ninth People's Congress, Dec. 28, 2000, *at* http://english.gov.cn/laws/2005–09/22/content_68771.htm [hereinafter Decisions]; Measures on Internet Information Services, State Council Order No. 292, Sept. 25, 2000, *translation available at* http://www.transasialawyers.com/translation/legis_16_e.pdf [hereinafter IIS Measures]; INTERNET FILTERING IN CHINA, *supra* note 48, at 9.

[56] Decisions, *supra* note 55, art. 2–4; IIS Measures, *supra* note 55, art. 15.

[57] Decisions, *supra* note 55, art. 2–4; IIS Measures, *supra* note 55, art. 15.

[58] IIS Measures, *supra* note 55, art. 7.

[59] *Id.* art. 14.

[60] *Id.*

[61] *Id.*

[62] Song Huang & Lingli Cheng, *Digital Divide New Rules on Internet News Information*, CHINA L. & PRAC., Dec. 2005, http://www.chinalawandpractice.com/default.asp?Page=1&cIndex=2&SID=4869&M=12&Y=2005.

[63] *Id.*

[64] *Id.*

news about current and political affairs must be the information released by official government news agencies.[65] Moreover, it is widely believed that the law is written broadly enough to encompass bloggers who post non-approved information.[66]

Providers of electronic messaging and bulletin board services must abide by their own set of restrictive rules.[67] Under the "Administration of Internet Electronic Messaging Provisions," all must obtain government approval before offering those services and must post their permit number, their messaging rules, and warnings about the liability they and users bear for the posting of restricted information.[68] Censors must be employed to ensure that the content of bulletin boards and chat room messages comply with government restrictions.[69]

These electronic messaging restrictions were recently augmented by new regulations designed to prevent spam.[70] The new provisions require users to enter true information about their identities when subscribing for e-mail addresses and mandate that the e-mail provider retain all sign-on and access records for sixty days.[71]

Operators of cybercafés are also singled out for special treatment under Chinese law.[72] Following a deadly cybercafé fire in 2002, the government imposed strict safety and licensing requirements for café owners.[73] Included in the new regulations were provisions prohibiting operators and users from using the cafés to access any of the categories of materials deemed inappropriate by the laws detailed above.[74] Technical measures must be installed to detect users who access illegal information and those users must be reported to the authorities.[75] The creden-

---

[65] *Id.*

[66] *Id.*

[67] *See* Administration of Internet Electronic Messaging Services Provisions, State Council, Oct. 27, 2000, *translation available at* http://www.chinalawandpractice.com/default.asp?Page=1&cIndex=2&SID=707&M=1&Y=2001.

[68] *Id.* arts. 8, 10.

[69] Kalathil & Boas, *supra* note 18, at 26.

[70] *See* Internet Society of China, China to Regulate Internet Email Services, Apr. 7, 2006, http://www.isc.org.cn/20020417/ca346007.htm; Sumner Lemon, *China's MII Publishes New E-mail Regulations,* NetworkWorld, Mar. 8, 2006, http://www.networkworld.com/news/2006/030806-china-e-mail-regulations.html.

[71] Internet Society of China, *supra* note 70; Lemon, *supra* note 70.

[72] *See* Newbold, *supra* note 54, at 510; Regulations on Administration of Business Premises for Internet Access Services, State Council, Sept. 29, 2002, *available at* http://english.gov.cn/laws/2005–07/25/content_16964.htm [hereinafter Cybercafé Rules].

[73] *See* Newbold, *supra* note 54, at 510.

[74] Cybercafé Rules, *supra* note 72, art. 14.

[75] *Id.* art. 19.

tials of all users must be checked and registered, along with that user's log-on information.[76] These records must be kept for 60 days.[77]

Finally, the Chinese government has created a voluntary "Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry" as well as a system by which citizens can report sites containing illegal information.[78] The Pledge requires the Internet company to monitor the information published by users, refrain from producing any prohibited information, remove harmful information, and refrain from establishing links to websites that contain harmful information.[79] The reporting system consists of a website through which Internet users can inform government censors of any illegal content they discover online.[80]

2. Technical Barriers

China backs up its extensive system of regulations with extensive technical control of its network.[81] Development of the Chinese Internet system has been controlled by the government from its inception.[82] In 1996, early in the network's development, the government group in charge of development decided to create a two-tiered system of Internet access. One tier is available for the public.[83] ISPs connect to this tier and provide access services to their customers.[84] This first tier, however, is only able to access the greater Internet outside the country through a second tier of the network.[85] This second tier is completely controlled by the State and thus provides government control over the borders between the Chinese Internet and the rest of

---

[76] *Id.* art. 23.

[77] *Id.*

[78] *See* Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry, Internet Society of China, July 19, 2002, *available at* http://www.isc.org.cn/20020417/ca102762.htm [hereinafter Pledge]; *Cyberspace Regulator Meets the Press,* China Internet Information Center, Feb. 17, 2006, http://service.china.org.cn/link/wcm/Show_Text?info_id=158424&p_qry=Liu%20and%20Zhengrong (discussing the "China Reporting Center of Illegal and Unhealthy Information").

[79] Pledge, *supra* note 78, art. 9.

[80] *See Cyberspace Regulator Meets the Press, supra* note 78.

[81] *See* Internet Filtering in China, *supra* note 48, at 3.

[82] *See* Kalathil and Boas, *supra* note 18, at 21.

[83] *Id.*

[84] *Id.*

[85] *See id.*

the world.[86] This plan has effectively made the entire country's network into one big intranet.[87]

The Chinese network backbone is comprised of some of the most powerful and advanced network technology available in the world. The OpenNet Initiative's 2004–05 study of Chinese Internet filtering reported that the Cisco 12000 series routers used in the network's backbone have dynamic packet filtering capabilities that allow the application of up to 750,000 bi-directional packet filtering rules.[88] It also appears that the government is using firewall and other network security software to selectively block data.[89]

With all of this technology at work, China's ability to censor information is extensive.[90] OpenNet Initiative's testing revealed that websites with information about Falun Gong, Tibetan Independence, and Taiwan were consistently inaccessible from within the country.[91] It found evidence of the interception of e-mail containing sensitive data, although this technology seemed less mature—filtering success largely depended on the language and character encoding used in the messages.[92] Messages submitted to online chat rooms were frequently excluded or removed if they contained sensitive information, and web sites that contained sensitive topics were excluded from the search results on China's largest search engines.[93] Clearly the country has enormous censorship ability and does not hesitate to use it.[94]

---

[86] *Id.*

[87] Newbold, *supra* note 54, at 511. An intranet is an Internet-like network that is separated from the rest of the Internet. Most organizations with computer networks employ an intranet design to facilitate intra-organization information sharing and to protect their computers from users on the rest of the Internet. *See* Webopedia, Intranet, http://www.webopedia.com/TERM/i/intranet.html (last visited May 6, 2007).

[88] Internet Filtering in China, *supra* note 48, at 7. Dynamic packet filtering technology enables an Internet router or firewall to examine individual TCP/IP data packets as they pass through the device and exclude those that the router administrator has identified in the router's "rules." These rules can restrict entire Internet protocols or packets coming from or going to specified Internet domains, IP addresses, or URLs containing certain words or phrases. *See* Webopedia, Stateful Inspection, http://www.webopedia.com/TERM/S/stateful_inspection.html (last visited May 7, 2007).

[89] *See* Internet Filtering in China, *supra* note 48, at 23–27.

[90] *See id.* at 23.

[91] *See id.* at 23–27.

[92] *See id.* at 46–47.

[93] *See id.* at 49, 51.

[94] *See* Internet Filtering in China, *supra* note 48, at 52.

C. *Foreign Assistance*

Although China certainly has capable engineers within its own country, experts agree that it could not have developed its system of monitoring and filtering without the help of Western hardware and software companies.[95] In fact, many countries that filter Internet content have taken advantage of products from U.S. companies.[96] Testing by the OpenNet Initiative has shown that SmartFilter software made by the U.S. company Secure Computing is used by government filters in Tunisia, Iran, the United Arab Emirates, and Saudi Arabia.[97]

As noted above, routers and switches manufactured by Silicon Valley based Cisco Systems (Cisco) comprise a large part of the Chinese Internet backbone and Internet filtering technology.[98] By one estimate, the company earns $500 million per year in China.[99] California computer giant Sun Microsystems and web-monitoring software maker Websense have also been implicated in sales of web filtering and monitoring technology to China.[100]

In the past few years, Internet companies have entered the Chinese playing field and have recently made headlines for the assistance they have provided to the censorship program.[101] Well before the enactment of the "Rules on the Administration of Internet News Information Services," U.S. companies providing e-mail, SMS, or Internet portal services such as Yahoo!, Microsoft, and Google, were already participating in the censorship of information.[102]

In mid-2002, Yahoo! signed China's "Public Pledge on Self-discipline for the Chinese Internet Industry" and voluntarily agreed

---

[95] *See* Lee, *supra* note 15; MacKinnon, *supra* note 14.

[96] Bambauer, *supra* note 48, at 56. *See generally* INTERNET FILTERING IN IRAN, *supra* note 47; INTERNET FILTERING IN SAUDI ARABIA, *supra* note 36; OPENNET INITIATIVE, INTERNET FILTERING IN TUNISIA IN 2005, *available at* http://www.opennetinitiative.net/tunisia; OPENNET INITIATIVE, INTERNET FILTERING IN THE UNITED ARAB EMIRATES IN 2004–2005, Feb. 2005, *available at* http://www.opennetinitiative.net/studies/uae/ONI_UAE_Country_Study.pdf.

[97] Bambauer, *supra* note 48, at 56.

[98] *See id.*, at 56; INTERNET FILTERING IN CHINA, *supra* note 48, at 7.

[99] *See* INTERNET FILTERING IN CHINA, *supra* note 48, at 7.

[100] Hu, *supra* note 14.

[101] *U.S. Task Force Eyes Net Censorship in China, Elsewhere*, CNET NEWS.COM, Feb. 14, 2006, http://news.com.com/U.S.+task+force+eyes+Net+censorship+in+China%2C+elsewhere/2100–1028_3–6039414.html

[102] *See* HUMAN RIGHTS WATCH, U.S.: PUT PRESSURE ON INTERNET COMPANIES TO UPHOLD FREEDOM OF EXPRESSION, Feb. 1, 2006, *available at* http://hrw.org/english/docs/2006/02/01/china12592.htm (presenting testimony of Tom Malinowski before the Congressional Human Rights Congress) [hereinafter Malinowski Testimony].

to refrain from establishing links to prohibited websites or disseminating "harmful information."[103] Since that time, Yahoo!'s search engine has returned restricted search results to Chinese users without informing them of any limitations.[104]

In 2005, soon after the enactment of the "Rules on the Administration of Internet News Information Services," Yahoo! provided the Chinese government with information that linked the IP address of Shi Tao's computer to an e-mail the Chinese government found objectionable.[105] The "state secret" leaked in the e-mail was information about government reporting guidelines for the commemoration of the fifteenth anniversary of the Tiananmen Square massacre.[106] Shi was sentenced to a ten year prison term for releasing it.[107]

Google initially resisted the Chinese censorship system and China blocked access to the site in early 2002.[108] Although it continued to resist censorship, Google was eventually unblocked.[109] In 2004, however, Google began to provide a version of Google news to China that excluded links to publications the Chinese government found objectionable.[110]

On January 24, 2006, Google announced its own limited Internet search engine, Google.cn, that would be hosted in China.[111] The site's search results only display links to sites to which the Chinese government does not object.[112] Although the search engine informs users that the search results have been censored, its technology actually excludes more information than the Yahoo! site and local Chinese search engines.[113] To avoid collecting user-identifying information, the site lacks the e-mail and blogging capabilities of Google.com and

---

[103] *See* Newbold, *supra* note 54, at 511, 513.

[104] Marc Gunther, *Yahoo's China Problem,* CNNMONEY.COM, Feb. 22, 2006, http://money.cnn.com/2006/02/21/news/international/pluggedin_fortune/.

[105] Kerstetter, *supra* note 5.

[106] *Id.*

[107] *Id.*

[108] Will Knight, *Google Mirror Beats Great Firewall of China,* NEWSCIENTIST.COM, Sept. 6, 2002, http://www.newscientist.com/article.ns?id=dn2768.

[109] *See* Reporters Without Borders, Google-Yahoo Market Battle Threatens Freedom of Expression, July 26, 2004, http://www.rsf.org/article.php3?id_article=11031.

[110] Malinowski Testimony, *supra* note 102.

[111] Barboza, *supra* note 6.

[112] *Id.*

[113] OpenNet Initiative Blog, Google.cn Filtering: How It Works, http://www.opennetinitiative.net/blog/?p=87 (last visited May 7, 2007).

also lacks the caching functionality that would allow Chinese users access to unblocked cached versions of prohibited websites.[114]

Microsoft has also helped censor Internet information.[115] When its online blog service, MSN Spaces, became available in China in May 2005 through servers in Shanghai, users discovered that the use of the words democracy, freedom, human rights, or demonstration in their postings returned an error message indicating that their "item contained forbidden speech."[116]

In December 2005, Microsoft removed the blog of Zhao Jing from MSN Spaces at the request of the Chinese government.[117] Zhao, also known as Michael Anti on his blog, was well known to the Chinese government.[118] He had frequently posted political commentaries by Chinese writers and had already been blocked for posting a letter critical of the editor of the China Youth Daily in a blog.[119] Microsoft not only removed Zhao's blog, but likely did so from a server within the United States.[120] That a U.S. company would comply with censorship demands and remove content from U.S.-hosted servers finally angered Congress into taking action.[121]

II. Discussion

Over the past several years, developments in law have left open the question of whether U.S. Internet companies can be held liable for violations of foreign Internet censorship laws.[122] At the same time, there have been legislative attempts to define the U.S. government's role in this area and limit the assistance U.S. companies can provide to Internet censoring countries.[123]

---

[114] Barboza, *supra* note 6, at C3; Malinowski Testimony, *supra* note 102.

[115] Barboza & Zeller, *supra* note 1, at C3; Donoghue, *supra* note 1.

[116] Donoghue, *supra* note 1; Malinowski Testimony, *supra* note 102.

[117] Barboza & Zeller, *supra* note 1, at C3; Donoghue, *supra* note 1.

[118] Hamish McDonald, *China's Web Censors Struggle to Muzzle Free-spirited Bloggers,* Sydney Morning Herald (Austl.), Dec. 23, 2005, *available at* http://smh.com.au/news/technology/chinas-web-censors-struggle-to-muzzle-freespirited-bloggers/2005/12/22/1135032135897.html.

[119] *Id.*

[120] Donoghue, *supra* note 1.

[121] Anne Broache & Declan McCullagh, *Congress Looks Askance at Firms That Bow to China,* CNET News.com, Jan. 12, 2006, http://news.com.com/Congress+looks+askance+at+firms+that+bow+to+China/2100–1028_3–6026733.html.

[122] *See* Marc H. Greenberg, *A Return to Lilliput: The* LICRA v. Yahoo! *Case and the Regulation of Online Content in the World Market,* 18 Berkeley Tech. L.J. 1191, 1205 (2003).

[123] *See, e.g.*, Broache & McCullagh, *supra* note 120; MacKinnon, *supra* note 14.

A. *Internet Jurisdiction*

U.S. companies argue that they must comply with foreign governments' demands if they want to conduct business in foreign countries.[124] Their compliance, however, may stem more from a desire to avoid liability for violation of foreign laws.[125] Such a fear is not unfounded after two French groups brought a lawsuit against Internet giant Yahoo!.[126]

In April 2000, *La Ligue Contre Le Racisme et L'Antisemitisme* (LICRA) sent a cease and desist letter to Yahoo!'s Santa Clara, California headquarters which threatened legal action unless the Internet company stopped providing access to sites selling Nazi paraphernalia.[127] Five days later, LICRA commenced such a lawsuit against Yahoo! and Yahoo! France in the Tribunal de Grande Instance de Paris.[128] The suit was joined by *L'Union des Etudiants Juifs de France* (UEJF).[129]

The suit claimed that Yahoo! had violated section R645–2 of the French Penal Code, which bans the exhibition of Nazi paraphernalia for sale and prohibits French citizens from purchasing or possessing such material.[130] Although Yahoo! operated a subsidiary in France, fr.yahoo.com, which removed such content, other Yahoo! servers hosted auction sites on which these materials were offered for sale.[131] These sites were accessible to anyone, including users in France, who entered Yahoo! through its main portal www.yahoo.com.[132]

The French court issued an interim order on May 22, which required Yahoo! to "take all necessary measures to dissuade and render impossible any access via yahoo.com to the auction service for Nazi merchandize as well as to any other site or service that may be construed as an apology for Nazism or contesting the reality of Nazi crimes," and imposed monetary penalties for each day of delay or

---

[124] *See* MacKinnon, *supra* note 14.

[125] *See* Goldsmith & Wu, *supra* note 15, at 44.

[126] *See id.* at 40.

[127] Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme (Yahoo IV), 433 F.3d 1199, 1202 (9th Cir. 2006).

[128] *Id.*

[129] *Id.*

[130] Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme (Yahoo III), 379 F.3d 1120, 1121 (9th Cir. 2004).

[131] *See id.* at 1121–22.

[132] *Yahoo IV,* 433 F.3d at 1202; *Yahoo III,* 379 F.3d at 1121–22.

confirmed violation.[133] Yahoo! objected to this order, contending that there was no technical solution that would allow it to fully comply.[134]

After commissioning an expert study of the situation, the court found that it was possible to determine a web surfer's country of origin with about seventy percent certainty.[135] Making particular reference to the fact that it appeared that Yahoo! was already using some of this technology, the court upheld its earlier interim order on November 6, 2000.[136] This new interim order kept the monetary penalties of the May order intact and added a provision requiring fr.yahoo.com to display a warning to surfers before they were able to link to www.yahoo.com.[137] The decision, however, declared that Yahoo! France, through actions taken after the initial order, had already "complied in large measure with the spirit and letter" of the May 22 order.[138]

The court did not impose the penalties of the order and LICRA and UEJS did not attempt to convince the court to do so.[139] Instead, the two groups claimed that they would only seek to have the penalties imposed if Yahoo! "revert[ed] to their old ways and violat[ed] French law."[140] At the time of this writing, neither plaintiff has sought enforcement of the penalties.

In late 2000, Yahoo! filed suit in federal district court in California.[141] The suit sought a declaratory judgment that the interim orders were not enforceable in the United States.[142] That court determined it had personal jurisdiction over the French groups and later determined enforcement of the orders was not mandatory and that a U.S. court does not have to give effect to foreign judicial orders if those orders violate American public policy or fundamental interests.[143] The

---

[133] *Yahoo IV*, 433 F.3d at 1202–03.

[134] *Id.* at 1203.

[135] *Id.*; UEJF et LICRA v. Yahoo et Yahoo France, [Interim Court Order of Nov. 20, 2000], Paris Tribunal de Grande Instance, No. RG: 00/05308, *available at* http://www.cdt.org/speech/international/001120yahoofrance.pdf; Goldsmith and Wu, *supra* note 15, at 43.

[136] *UEJF et LICRA*, No. RG 00/05308. The expert report noted that web users visiting www.yahoo.com from computers located within France were greeted with French advertising. *Id.*

[137] *Id.*

[138] *Yahoo IV,* 433 F.3d at 1204.

[139] *Id.*

[140] *Id.*

[141] Greenberg, *supra* note 122, at 1227–28.

[142] *Yahoo IV*, 433 F.3d at 1204.

[143] Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme (Yahoo II), 169 F. Supp. 2d 1181, 1189 (N.D.Cal. 2001); Yahoo!, Inc. v. La Ligue Contre Le Racisme et

French orders were found to violate Yahoo!'s fundamental rights under the First Amendment and were declared unenforceable.[144]

LICRA and UEJF appealed to the Ninth Circuit and a three justice panel found that the district court erred in finding personal jurisdiction over the two organizations.[145] The court granted rehearing en banc and reversed the panel's holding of lack of jurisdiction.[146] The case was dismissed, however, because, of the eleven judges, a three judge plurality did not find Yahoo!'s First Amendment claim ripe for adjudication and another three judges found no personal jurisdiction.[147]

In short, the French injunction against Yahoo! remains in effect and the question remains unanswered whether it or any other order forcing a U.S. company to comply with foreign Internet censorship laws is a violation of the First Amendment.[148] It appears that an actual attempt by a foreign government to impose damages would not be enforced, but injunctions that restrict the kinds of information foreign web surfers can access from those countries may be enforceable.[149] Google, Microsoft, and the other companies doing business in China may be forced, by threat of injunction, to comply with Chinese court orders limiting the kind of content available to Chinese surfers.[150]

B. *Global Internet Freedom Act*

The "Global Internet Freedom Act" (GIFA) was first introduced in the House and Senate in October 2002.[151] Nearly identical versions of the bill were introduced in 2003, 2005, and 2006, but not one has been enacted.[152] The purpose of the Act, as stated in its most recent iteration, is "to develop and deploy technologies to defeat 'Internet jam-

---

L'Antisemitisme (Yahoo I), 145 F. Supp. 2d 1168, 1180 (N.D.Cal. 2001); Greenberg, *supra* note 121, at 1246.

[144] *Yahoo II*, 169 F. Supp. 2d at 1194.

[145] Yahoo! Inc. v. La Ligue Contre Le Recisme et L'Antisemitisme (Yahoo III), 379 F.3d, 1120, 1126 (9th Cir. 2004).

[146] *Yahoo IV*, 433 F.3d at 1224.

[147] *Id.*

[148] *See id.* at 1252 (Fisher, J., dissenting).

[149] *See id.* at 1223–24.

[150] *See id.* at 1252 (Fisher, J., dissenting).

[151] S. 3093, 107th Cong. (2002); H.R. 5524, 107th Cong. (2002).

[152] *See* H.R. 4741, 109th Cong. (2006); H.R. 2216, 109th Cong. (2005); H.R. 48, 108th Cong. (2003).

ming.'"[153] If passed, it would establish the Office of Global Internet Freedom (OGIF) within the International Broadcasting Bureau (IBB), which would work to develop and implement a comprehensive global strategy to combat the state-sponsored and state-directed "Internet-jamming" and user persecution conducted by repressive foreign governments.[154]

The idea behind the Act stems from the historical activities of the U.S. Foreign Information Service (FIS).[155] The FIS, now the IBB, was created in 1941 and began broadcasting the Voice of America (VOA) during World War II.[156] For much of its existence, a large portion of VOA's operating funds have been spent on technologies to prevent repressive governments from jamming the transmission of news from VOA, Radio Free Asia, and other news sources.[157]

The IBB already deploys some technology to counter Internet-jamming, but the Act would significantly increase the volume of this activity.[158] At the date of the latest introduction of the Act, the VOA and Radio Free Asia had spent only $3 million on Internet counter-jamming technology.[159] The Act would establish a budget of $50 million for the OGIF.[160] The OGIF would be specifically authorized to work with the private sector to acquire and implement the technology necessary to defeat Internet blocking and censorship.[161]

C. *Global Online Freedom Act*

The latest legislative response to Internet censorship is the "Global Online Freedom Act of 2006" (GOFA).[162] This bill was introduced in February 2006 at the close of the House Subcommittee hearings on Chinese Internet censorship.[163] It incorporates elements of GIFA, but extends that bill to include stiff civil and criminal penal-

---

[153] H.R. 4741 § 6 defines "Internet jamming" as "jamming, censoring, blocking, monitoring, or restricting Internet access and content by using such technologies as firewalls, filters, and 'black boxes.'"

[154] H.R. 4741 § 4(a).

[155] *See* Chen, *supra* note 18, at 233–35.

[156] *Id.* at 234–35.

[157] *Id.* at 235.

[158] *See* H.R. 4741 §§ 2(9), 3.

[159] *Id.* § 2(9).

[160] *Id.* § 4(e).

[161] *Id.* § 3(5).

[162] H.R. 4780, 109th Cong. (2006).

[163] Rebecca MacKinnon, *America's Online Censors,* THE NATION.COM, Mar. 13, 2006, http://www.thenation.com/doc/20060313/mackinnon [hereinafter *America's Censors*].

ties for U.S. companies that offer assistance to governments that censor, block, monitor, or restrict access to the Internet.[164]

Like GIFA, GOFA would create an Office of Global Internet Freedom to develop and implement a global strategy to counter Internet blocking and censoring by foreign governments.[165] Unlike GIFA, the GOFA OGIF would be part of the Department of State and would ultimately report to the President.[166] It would develop a strategy to combat Internet censorship, but would also work with the President to create an annual report of countries that restrict Internet access and the methods by which that restriction is achieved.[167]

With information supplied by the OGIF, the President would determine which countries were directly or indirectly responsible for restricting Internet freedom and would provide an annual list of designated "Internet-restricting" countries to Congress.[168] The GOFA would initially designate Burma, China, Iran, North Korea, Tunisia, Uzbekistan, and Vietnam to this list.[169]

U.S. companies could not host a search engine in a country designated Internet-restricting.[170] They could not alter the search results of their U.S.-hosted search engines to satisfy the laws of foreign countries, and they would have to provide the OGIF with any and all terms and parameters that any foreign country uses to filter its results.[171] Content hosts could restrict access to content at the request of foreign Internet-restricting governments, but would be required to provide a list of any content removed or blocked to the OGIF.[172] Finally, no U.S. business could provide any official from an Internet-restricting country with information that could personally identify a particular user of that company's services.[173]

The GOFA would create a private right of action in U.S. courts for citizens of Internet-restricting countries whose personal information is revealed to their governments.[174] These civil suits could result

---

[164] *See* H.R. 4780 § 207.
[165] *Id.* § 104(a).
[166] *Id.* § 104(a)–(b).
[167] *Id.* § 104(b)(3).
[168] *Id.* § 105.
[169] H.R. 4780 § 105(a)(3).
[170] *Id.* § 201.
[171] *Id.* § 203.
[172] *Id.* § 205.
[173] *Id.* § 206(a).
[174] H.R. 4780 § 206(b).

in damage awards of up to $2 million.[175] Additional criminal penalties would result in fines against companies and up to five years imprisonment for individuals convicted of information disclosure.[176]

The Attorney General could bring civil suits for violation of the search engine and content host provisions of the Act, which could result in penalties of up to $10,000.[177] Individuals violating these provisions would face criminal fines and up to one year in prison.[178]

Finally, the GOFA would establish controls on exports and licensing of hardware and software.[179] The Act would require the promulgation of regulations preventing the knowing export of items used in Internet censorship to "Internet-restricting" countries.[180]

III. Analysis

While at first glance the GOFA appears to address the issue of Internet censorship head-on and punish those companies that assist Internet-restricting governments,[181] upon closer inspection several troubling details arise. A thoughtful analysis reveals that the bill, if enacted as is, would go too far in its policing efforts while at the same time do too little to curb international Internet censorship.

A. *Excessive Provisions*

The first troubling aspect of GOFA lies in its definition of a "United States Business."[182] The bill includes companies that are incorporated in the United States, subsidiaries of those companies, and "any issuer of a security registered pursuant to section 12 of the Securities Exchange Act of 1934."[183] This means that any company listed on one of the U.S. security exchanges could be found liable in a U.S. court.[184] Tom Online, Sohu.com, and Baidu.com, the leading Chinese search engine, are all Chinese companies listed on the NASDAQ exchange

---

[175] *Id.* § 207(a).
[176] *Id.* § 207(b).
[177] *Id.* § 207(a)(2).
[178] *Id.* § 207(b)(2).
[179] H.R. 4780 § 301.
[180] *Id.* § 301.
[181] *See supra,* Part II(C).
[182] *See* H.R. 4780 § 3(11).
[183] *Id.*
[184] Chris Myrick, *FOCUS-Proposed 'Online Freedom Act' May Hurt US and US-Listed China Firms,* Forbes.com, Feb. 16, 2006, http://www.forbes.com/afxnewslimited/feeds/afx/2006/02/16/afx2531410.html.

and could face U.S. lawsuits if the GOFA is enacted.[185] Whether any damages in such suits could be enforced is questionable after *Yahoo! v. LICRA*, but the uncertainty would be damaging to those companies and their U.S. financial backers.[186] Faced with the choice of breaking either local laws or U.S. laws, these companies would simply de-list themselves from NASDAQ and join either the Shanghai exchange or the Hong Kong Bourse.[187] This would do nothing to curb censorship and would hurt the NASDAQ and its U.S. investors.[188]

Another cause for concern is the section of the Act that forces U.S. companies to report any content they have been asked to block or remove from their servers.[189] While a case can be made that the U.S. government needs to know what kind of content is censored in order to create effective countermeasures to Internet restrictions, this provision goes too far.[190] By obtaining the content of blogs, e-mail, and websites blocked by foreign countries, OGIF would obtain exactly the kind of personal information about Internet users that it would work to prevent other countries from learning.[191] This result could lead to distrust of the OGIF and the U.S. government.[192]

A third area in which the GOFA causes concern is its list of Internet-restricting countries.[193] The OGIF would compile data about countries' Internet censorship activities and consult with private companies and non-government organizations for assistance, but it would be the President, with no discernable guidelines to follow, who would decide which countries were on the list.[194] The implications of this system are troubling.

First, businesses selling products to foreign countries would be hurt financially.[195] Not only would they be prevented from selling any products that have the potential to aid in censorship to Internet-restricting countries, but they might also be unable to enter into multi-year contracts to supply these products or support services to any coun-

---

[185] *Id.*
[186] *See id.*
[187] *Id.*
[188] *See id.*
[189] *See* H.R. 4780 § 205.
[190] *See America's Censors,* supra note 163.
[191] *See id.*
[192] *See id.*
[193] *See* H.R. 4780 § 105.
[194] *See id.* §§ 104, 105.
[195] *See id.* § 301.

try.[196] With the possibility of arbitrary inclusion of any country to the list, a company could find itself breaking the law by fulfilling its contract obligations in a country that was not on the list at the time of the agreement, but was included later.

Second, the list has the potential to be politically motivated. The interests of goodwill or positive foreign relations could easily trump the goal of reducing Internet censorship abroad. Indeed the makeup of the initial list of Internet-restricting countries already reveals this sort of political favoritism.[197] The initial countries include communist regimes and countries hostile to the United States, while other countries that have strict Internet censorship laws, but are financially important to the United States, such as Saudi Arabia and the United Arab Emirates, are conspicuously absent.[198]

B. *Ineffective Measures*

While the GOFA is excessive in many of its provisions,[199] it still manages to be relatively ineffective at preventing Internet blocking and censorship. If the goal of the Act is to promote free speech and the free exchange of information, portions of the Bill must be changed.

The first area in which the Act is ineffective is in its definition of which companies are subject to liability.[200] As discussed above, the Bill is over-inclusive in that it includes companies that do no business within the United States.[201] At the same time, it is under-inclusive in that some U.S. companies that have already caused harm would not be affected.[202] Yahoo!, because of its disclosure of the identity of Shi Tao, is arguably the worst offender of any company that has assisted Chinese censorship.[203] Yahoo!, however, would not be held liable for its transgressions under the GOFA.[204] Yahoo.cn, the entity that revealed the information to Chinese government authorities, is a subsidiary of Yahoo!, but the Chinese company Alibaba.com owns sixty percent of that subsidiary.[205] Alibaba is not listed on a U.S. securities

---

[196] *See id.*
[197] *See* H.R. 4780 § 105(a)(3).
[198] *See id.*
[199] *See supra* Part III(A).
[200] *See* H.R. 4780 § 3(11).
[201] *See* Myrick, *supra* note 183.
[202] *See id.*
[203] *See* Gunther, *supra* note 104; *America's Censors, supra* note 163.
[204] *See* Myrick, *supra* note 184.
[205] *Id.*

exchange and, by virtue of this controlling interest, both it and Yahoo! would escape liability.[206]

Another way the GOFA fails to achieve its goal of promoting global freedom of information is through its method of designating "Internet-restricting" countries.[207] As discussed above, companies would only be prohibited from assisting countries designated as Internet-restricting by the President.[208] The initial list of countries already has glaring omissions and it is likely that countries that censor will remain excluded from the list either for political reasons or because their censorship is simply not as egregious as that of other offenders.[209] While the GOFA will have some effect on China and other countries that make the list, the citizens of restricting countries not included will have no recourse for any harm.[210]

In sum, the GOFA, while touted as a bill to promote and protect global Internet freedom, has several troubling provisions and does little to actually promote free world-wide information exchange.[211] It seems designed to be more a form of punishment for U.S. companies that have already assisted Internet-censoring governments than a real attempt to prevent censorship altogether.[212] More work must be done and more thought put into this Bill.[213]

C. *What Can Be Done?*

If the GOFA fails to accomplish its goal of preventing censorship, what can be done? In an open letter to the members of the Subcommittee on Africa, Global Human Rights, and International Operations, at the beginning of that committee's February hearings, the Electronic Frontier Foundation (EFF) laid out a number of topics for the committee to discuss with the Internet companies in attendance.[214] When combined with several provisions of the Global Information Freedom

---

[206] *See id.*

[207] *See* H.R. 4780 § 105.

[208] *Id.* § 301.

[209] *See supra,* Part III(A).

[210] *See* H.R. 4780 § 207.

[211] *See supra* Part III(A) and (B).

[212] *See, e.g.,* Myrick, *supra* note 184.

[213] *See, e.g., America's Censors, supra* note 163.

[214] Electronic Frontier Foundation, A Code of Conduct for Internet Companies in Authoritarian Regimes, Feb. 15, 2006, http://www.eff.org/deeplinks/archives/004410.php [hereinafter Code of Conduct].

Act, these topics should serve as the foundation for an effective new U.S. response to the problem of Internet censorship.[215]

1. Limit Data Collection and Data Retention

Information that could personally identify a particular user of Internet services is the most dangerous information Internet companies possess.[216] In countries such as China, even the IP address of a computer accessing restricted information may be enough to identify the person operating that computer.[217] To the extent possible, Internet service providers should refrain from collecting and storing any such information that could personally identify individual users.[218]

In the search engine and content provider contexts, this could be as simple as storing IP address information in a way that completely dissociates the address information from the search conducted or content accessed.[219] In e-mail and instant messaging situations, the goal should be to collect as little information as is necessary to provide the service and to retain that information for as little time as possible.[220] If the information needed can easily identify a particular user, that information should be stored on servers outside of the restricting country.[221]

2. Incident Collection and Reporting

Internet companies should collect and publish statistics on the amount of information they have been asked to block or remove from their servers and the reasons given for these requests.[222] They should specifically note the particular law enforcement agency that requested the censorship and the law, if any, that was used to justify the action.[223]

If a search engine is required to censor search results or prevent access to sites, it should inform users that information has been ex-

---

[215] *See id.*

[216] *See id.*

[217] *See* IIS Measures, *supra* note 55, art. 14.

[218] *See* Code of Conduct, *supra* note 214.

[219] *See id.* Indeed, since this Note was written, Google has begun to remove such identifying information from the search data it retains in an effort to protect the identities of people making specific search requests. Michael Liedtke, *Google Tightens Privacy Measures to Shield Search Requests,* Law.com, March 15, 2007, http://www.law.com/jsp/article.jsp?id=1173863016070.

[220] *See id.*

[221] *See America's Censors, supra* note 163.

[222] *See id.*

[223] *See id.*

cluded from the results.[224] It should provide the URL for the excluded information even if that URL is unreachable from within the restricting country.[225] Information about such censorship requests should be collected, stored, and published.[226]

Collecting this data will provide valuable information for entities working to counteract the censorship activities of foreign countries and will provide the international community with evidence of the repressive nature of censorship regimes.[227] While the GOFA advocates this kind of collection, it only does so with countries on the Internet-restricting list and also requires collection of the specific content censored.[228] A better approach is to protect the rights and identities of individual Internet users by collecting this data from all countries, but reporting only the types of information excluded and the reasons for exclusion.[229]

3. Do not do Direct Business with Forces of State Oppression

The EFF next recommends that U.S. companies be prohibited from intentionally providing support and assistance to those who would restrict the free exchange of information on the Internet.[230] This does not mean, as the GOFA suggests, that companies should be barred from selling any products that can be used for such purposes to foreign countries.[231] Many of those products, such as Internet routers and firewall software, have legitimate purposes in protecting networks from hackers and preventing the spread of Internet viruses.[232] Preventing their use for legitimate purposes will only harm world-wide Internet users.[233]

With that said, there is still no need for U.S. companies to offer knowing assistance to foreign officials specifically requesting assistance

---

[224] *See* Reporters Without Borders, *supra* note 109.

[225] *See, e.g.*, Gunther, *supra* note 104.

[226] *See* Reporters Without Borders, *supra* note 109.

[227] *See id.*

[228] *See* H.R. 4780 §§ 203, 205.

[229] *See* CODE OF CONDUCT, *supra* note 214; *America's Censors, supra* note 163.

[230] *See* CODE OF CONDUCT, *supra* note 214; *America's Censors, supra* note 163.

[231] *See* H.R. 4780 § 301.

[232] *See* CODE OF CONDUCT, *supra* note 214.

[233] *See The Internet in China: A Tool for Freedom or Suppression?: Joint Hearing Before the Subcomm. on Africa, Global Human Rights and Int'l Operations*, 109th Cong. 77–80 (2006) (statement of Mark Chandler, Cisco Systems), *available at* http://www.foreignaffairs.house.gov/archives/109/26075.pdf.

with Internet censorship.[234] Companies should offer assistance for the legitimate uses of their products and no more.[235] Granted, this will be a difficult line to draw, as legitimate purposes and censorship uses often overlap.[236] Still, to the extent such a provision helps change the mindset of U.S. corporations, it will benefit the fight against Internet censorship.

4. Offer Opportunistic Encryption with Internet Services

The availability of opportunistic encryption is a crucial step in the promotion of free speech and free information exchange online.[237] Most online services transmit easily intercepted unencrypted plain-text data over the Internet.[238] Encryption provides a relatively easy way to make the same information unreadable and should be added to protect the content of e-mail messages, instant messaging, and search requests and results whenever possible.[239]

The potential problem with offering encryption lies in U.S. export controls that bar encryption exports to some foreign countries.[240] However, China and Saudi Arabia are not included in the list of embargoed countries.[241] The use of encryption would therefore aid the citizens of two of the strictest Internet censoring regimes, and serious consideration should be given to modifying the export rules to allow at least export strength encryption to be exported to embargoed countries.[242]

5. Support Technologies that Innovate Around Censorship and Surveillance

The final EFF suggestion is that governments and private companies should invest in and develop technologies to circumvent the censorship efforts of foreign governments.[243] By creating the OGIF within

---

[234] *See id.*

[235] *See id.*

[236] *See id.*

[237] *See* Code of Conduct, *supra* note 214.

[238] *Id.*

[239] *Id.*

[240] *See* Bureau of Industry and Security, U.S. Dept. of Commerce, Encryption License Exception Chart, Dec. 9, 2004, *available at* http://www.bis.doc.gov/encryption/lechart1.htm.

[241] 15 C.F.R. § 746 (2006) (listing embargoed countries).

[242] *See* Press Release, Electronic Frontiers Foundation, Civil Liberties Groups Say New Encryption Export Regulations Still Have Serious Constitutional Deficiencies, (Jan. 13, 2000), http://www.eff.org/Privacy/Crypto/20000113_eff_pr.php.

[243] *See id.*

the IBB, the GIFA not only creates a government office with that responsibility, but also puts control of that office in the hands of the organization that has spent decades developing and operating anti-radio jamming technologies for Radio Free America, Radio Free Europe, and Radio Free Asia.[244] Enacting this GIFA provision would provide substantial funding for cooperation with private companies in the development and deployment of technologies that would extend this anti-jamming mission to the Internet.[245]

6. Penalties

Although neither the EFF nor the GIFA recommend penalties for U.S. companies that assist in Internet censorship, such penalties will be an important aspect of any legislation seeking to curb U.S. companies' involvement in Internet censorship.[246]

Unlike the broad-based penalties recommended by the GOFA that would affect foreign companies that are merely listed on U.S. securities exchanges, U.S. legislation should focus on penalizing only U.S. companies and the foreign subsidiaries in which those companies own a controlling share.[247] Both civil and criminal remedies should be available against any such company or individual that reveals any information that could be used to identify users of their services.[248] These penalties would not only provide companies with a legitimate reason to refuse foreign demands for such information, but would also give this legislation the bite it needs to be an effective deterrent for U.S. companies.[249]

7. International Cooperation

Finally, the United States cannot solve the problem of Internet censorship by simply enacting domestic legislation.[250] It may be able to curb some activities of U.S. companies, but many foreign companies, including those within Internet-restricting countries, are ready and able to step into any void left by lessened U.S. competition.[251]

---

[244] *See* H.R. 4741 §§ 4(e), 2(8), 109th Cong. (2006).

[245] *See id.* § 4(e).

[246] *See* H.R. 4780 § 207.

[247] *See,* Myrick, *supra* note 184.

[248] *See* H.R. 4780 §§ 207(a)(1), 207(a)(2).

[249] *See id.*

[250] *See America's Censors, supra* note 163.

[251] *See* Declan McCullagh, *China: Web Censorship Gives US Pause for Thought,* SILICON.COM, Jan. 13, 2006, http://management.silicon.com/government/0,39024677,39155583,00.htm.

The United States must therefore work with the United Nations and foreign countries that share its desire to promote free expression to address the problem on a global scale and apply pressure to all nations that restrict the free exchange of information.[252] The GIFA already contains sections that call for a U.N. resolution and increased pressure from the international community.[253] Both of these provisions should be included in any U.S. legislation.[254]

III. Conclusion

Global Internet censorship is a problem that affects all those who cherish freedom of expression and the free exchange of ideas. The United States and other countries that value these rights need to work together to provide the appropriate pressures and incentives to open the Internet for all to use without restriction.

At the same time, countries pushing for censorship reform need to maintain the moral high ground. It is somewhat hypocritical, for example, for the United States to propose legislation preventing companies from providing user information to foreign governments at the same time that it presses those same companies to provide it with information about the Internet searches of U.S. Internet users.[255] Likewise, it should not criticize other countries for monitoring e-mail and instant messaging communications while it takes measures to make that same information more easily accessible for officials in this country.[256] The Internet should remain a conduit for free expression of all information, not that information approved by any one government. Only be achieved with global understanding and cooperation can this goal be achieved.

---

[252] *See* H.R. 4741 §§ 3(6), 5(2).

[253] *See id.*

[254] *See id.*; *America's Censors*, *supra* note 163.

[255] *See* Mohammed, *supra* note 27.

[256] Declan McCullagh, *Police blotter: Patriot Act E-mail Spying Approved,* CNET News.com, Feb. 10, 2006, http://news.com.com/2102–1030_3–6037596.html.