U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology

Patricia Moloney Figliola, Coordinator
Specialist in Internet and Telecommunications Policy

Kennon H. Nakamura
Analyst in Foreign Affairs

Casey L. Addis
Analyst in Middle Eastern Affairs

Thomas Lum
Specialist in Asian Affairs

April 5, 2010

Congressional Research Service
7-5700
www.crs.gov
R41120

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Modern means of communications, led by the Internet, provide a relatively inexpensive, open, easy-entry means of sharing ideas, information, pictures, and text around the world. In a political and human rights context, in closed societies when the more established, formal news media is denied access to or does not report on specified news events, the Internet has become an alternative source of media, and sometimes a means to organize politically.

The openness and the freedom of expression allowed through blogs, social networks, video sharing sites, and other tools of today's communications technology has proven to be an unprecedented and often disruptive force in some closed societies. Governments that seek to maintain their authority and control the ideas and information their citizens receive are often caught in a dilemma: they feel that they need access to the Internet to participate in commerce in the global market and for economic growth and technological development, but fear that allowing open access to the Internet potentially weakens their control over their citizens.

Legislation now under consideration in the 111th Congress would mandate that U.S. companies selling Internet technologies and services to repressive countries take actions to combat censorship and protect personally identifiable information. Some believe, however, that technology can offer a complementary and, in some cases, better and more easily implemented solution to some of those issues. They argue that hardware and Internet services, in and of themselves, are neutral elements of the Internet; it is how they are implemented by various countries that is repressive. Also, Internet services are often tailored for deployment to specific countries; however, such tailoring is done to bring the company in line with the laws of that country, not with the intention of allowing the country to repress and censor its citizenry. In many cases, that tailoring would not raise many questions about free speech and political repression.

This report provides information regarding the role of U.S. and other foreign companies in facilitating Internet censorship by repressive regimes overseas. The report is divided into several sections:

- Examination of repressive policies in China and Iran,
- Relevant U.S. laws,
- U.S. policies to promote Internet freedom,
- Private sector initiatives, and
- Congressional action.

Two appendixes describe technologies and mechanisms for censorship and circumvention of government restrictions.

Contents

Figures

Appendixes

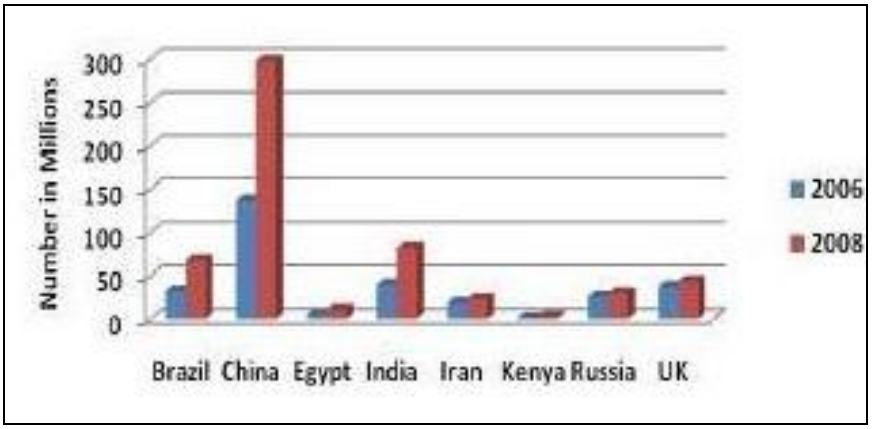
Contacts

Introduction

In the late 1960s and 1970s, advancements in telecommunications technologies enabled the creation of a large-scale, interconnected network called ARPANET ("Advanced Research Projects Agency Network"). ARPANET was created by the Defense Advanced Research Projects Agency as a government-funded enterprise until the mid-1990s, when it began commercialization. Today's Internet is a direct outgrowth of the technologies developed and lessons learned from ARPANET. During the late 1990s, the Internet began having a significant impact on culture and commerce, including the exponential increase of near instant communication by electronic mail (e-mail), text-based discussion forums, and the graphical World Wide Web.

Figure 1. Growth in Number of Internet Users in Select Countries

2006-2008



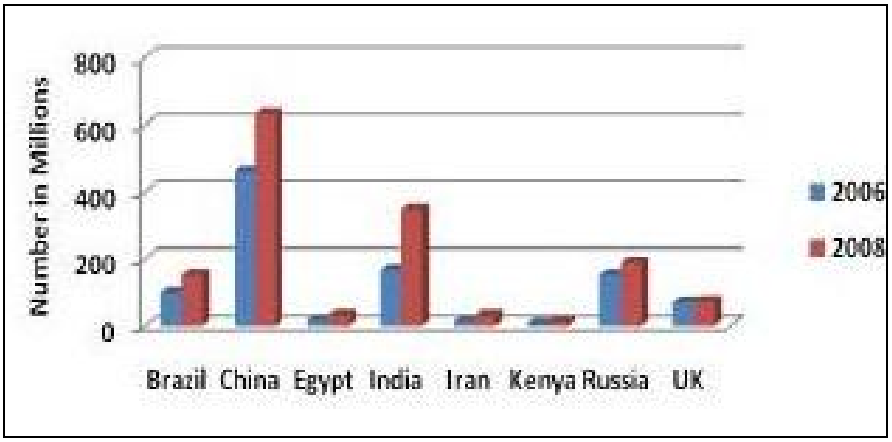
Source: : "Freedom on the Net: A Global Assessment of Internet and Digital Media," Freedom House, April 1, 2009.

Today, the Internet has evolved even further and many people are using newer tools, such as blogs, social networks, video sharing sites, and other aspects of today's communications technology to express their political ideals, many times in conflict with the political opinions and outlook espoused by their governments. In this way, the Internet has proven to be an unprecedented and often disruptive force in some closed societies, as the governments seek to maintain their authority and control the ideas and information their citizens receive. These regimes are often caught in a dilemma: they need the Internet to participate in commerce in the global market and for economic growth and technological development, but they also seek to restrict the Internet in order to maintain the government's control. **Figure 3** illustrates an assessment by Freedom House[1] of the extent to which selected countries restrict freedom on the Internet.

[1] Freedom House is an independent watchdog organization that supports the expansion of freedom around the world. Freedom House supports democratic change, monitors freedom, and advocates for democracy and human rights. More information can be found on its website, http://www.freedomhouse.com.

Figure 2. Growth in Mobile Phone Access in Select Countries

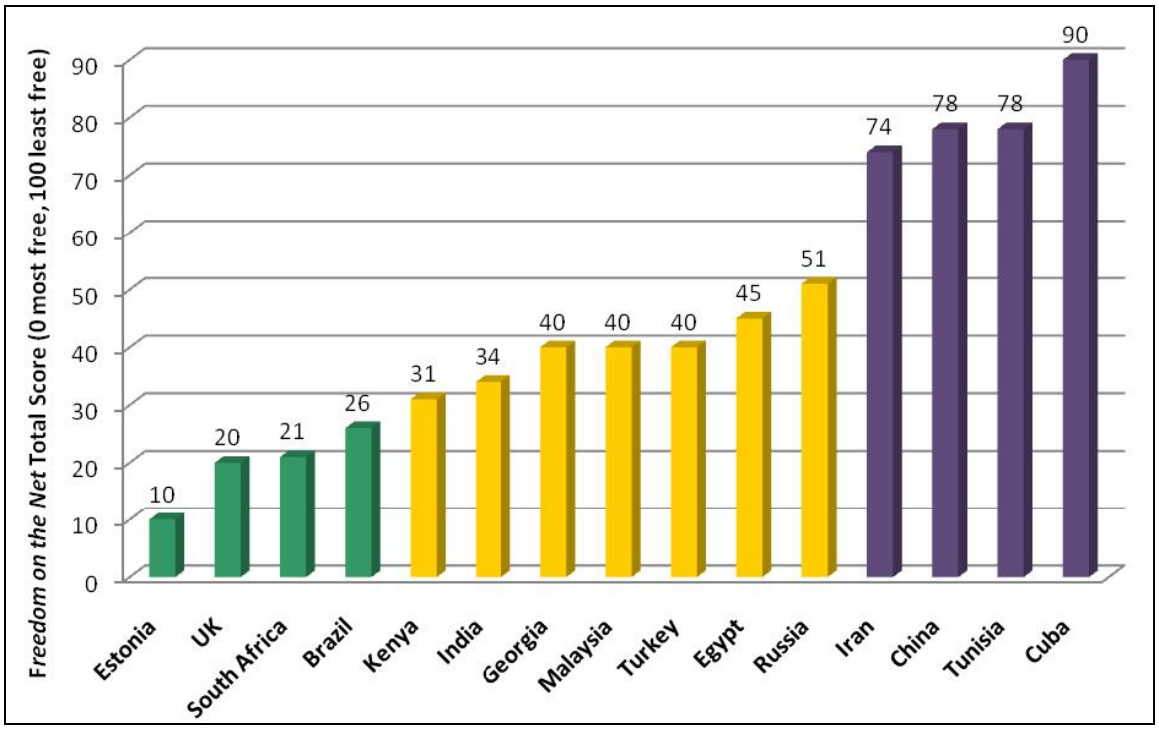
2006-2008



Source: "Freedom on the Net: A Global Assessment of Internet and Digital Media," Freedom House, April 1, 2009.

Figure 3. Freedom on the Net

15 Country Comparison (0 Best, 100 Worst)



Source: "Freedom on the Net: A Global Assessment of Internet and Digital Media," Freedom House, April 1, 2009

Notes: Estonia to Brazil are "Free." Kenya to Russia are "Partly Free." Iran to Cuba are "Not Free."

In Burma during the 2007 Saffron Revolution, YouTube footage, often filmed with cell phone cameras, conveyed to the world the human rights violations against the monks and generated international awareness and reaction. Demonstrations in Tehran following the June 12, 2009, presidential elections were often organized through Twitter and text messages over cell phones.

The Iranian government's violent response to the demonstrations was spread around the world through live cell phone pictures, e-mails, and phone calls. The Voice of America (VOA) reported that during the demonstrations, Iranians sent VOA over 300 videos a day, along with thousands of still pictures, e-mails, and telephone calls to the agency.[2]

A variety of control mechanisms are employed by regimes seeking to limit the ways the Internet is used, ranging from sophisticated surveillance and censorship to threats of retaliation (which foster self-censorship) and actual harassment and arrests of Internet users. Such regimes often require the assistance of foreign Internet companies operating in their countries. These global technology companies find themselves in a dilemma. They often must choose between following the laws and the requests of authorities of the host country, or refusing to do so and risking the loss of business licenses or the ability to sell services in that country. Human rights groups have protested that Yahoo! and Google censor and remove material deemed sensitive by host governments on country-specific search engines.[3] Microsoft is said to censor Chinese versions of its blog platforms.[4] Human rights groups also charge that Yahoo! has provided Chinese authorities personal identifying information about users that has allowed the government to identify and arrest individuals for statements made on the Web.[5] A representative of Google, Inc. acknowledged the problem of government involvement, noting

> As our ... Burma experiences indicate, our products are platforms for free expression, transparency, and accountability. Because of this, we often face efforts by governments throughout the world to restrict or deny access to our products.[6]

The Global Online Freedom Act of 2009 (GOFA) (H.R. 2271), introduced by Representative Christopher Smith, would mandate that companies selling Internet technologies and services to repressive countries take actions to combat censorship and protect personally identifiable information. Some believe, however, that technology can offer a complementary and, in some cases, better and more easily implemented solution to prevent government censorship. Hardware and Internet services, in and of themselves, are neutral elements of the Internet; it is how they are implemented by various countries that makes Internet access "repressive."

For example, hardware, such as routers, is needed to provide Internet service everywhere. However, hardware features intended for day-to-day Internet traffic management, conducted by Internet service providers (ISPs) and governments for benign purposes, can be misused. Repressive governments are able to use these features to censor traffic and monitor use—sometimes using them to identify specific individuals for prosecution. It is not currently feasible to remove those features from the product, even when sold to countries that use those features to repress political speech.[7]

---

[2] Danforth Austin, Director, Voice of America, testimony before the Subcommittee on Europe, House Committee on Foreign Affairs, Washington, July 23, 2009.

[3] Lucie Morillon, Washington Director of Reporters Without Borders, Testimony before the Tom Lantos Human Rights Commission, U.S. House of Representatives, Washington, June 18, 2009.

[4] Ibid.

[5] Ibid.

[6] Nicole Wong, Deputy General Counsel, Google, Inc., Testimony before the U.S. Senate Judiciary Committee's Subcommittee on Human Rights and the Law, Washington, May 20, 2008.

[7] Testimony of Mark Chandler, Cisco Systems, before the Senate Committee on the Judiciary Subcommittee on Human Rights and the Law, May 2, 2008.

On the other hand, Internet services, such as Google, are often tailored for deployment to specific countries. Such tailoring is done to bring the company's products and services in line with the laws of that country, and not with the end goal of allowing the country to repress and censor its citizenry. In many cases, tailoring does not raise many questions about free speech and political repression because the country is not considered to be a repressive regime. Under Canadian human rights law, for example, it is illegal to promote violence against protected groups; therefore, when reported, Google.ca will remove such links from search results.[8]

Internet censorship and the prosecution of individuals who attempt to circumvent that censorship are unlikely to be eliminated in some countries. However, while some governments are continually looking for new and more thorough methods to restrict or inhibit Internet use, citizens in these countries are active in developing techniques to circumvent those efforts.

Examples of Countries Charged with Restricting Internet Freedom

The organization Reporters Without Borders has listed 15 countries where Internet freedom is restricted. These countries are China, Cuba, North Korea, Belarus, Myanmar, Egypt, Ethiopia, Iran, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, Vietnam, and Zimbabwe.[9] This report covers two of these countries, China and Iran, both of which have been in the news during 2009 and 2010.

China[10]

The People's Republic of China (PRC) has the world's largest number of Internet users, estimated at 330 million people, including 70 million bloggers. It also has one of the most sophisticated and aggressive Internet censorship and control regimes in the world. According to some estimates, between 30 and 40 Chinese citizens are serving prison sentences for writing about politically sensitive topics online.[11] In November 2009, Huang Qi, a human rights advocate, was sentenced to three years in prison for "possessing state secrets" after posting online appeals and complaints of families whose children had been killed in school buildings during the Sichuan earthquake of May 2008. Some studies show that the vast majority of Internet users in China do not view the medium as a political tool.[12] Nonetheless, Chinese Internet users are able to access unprecedented amounts of information, despite government attempts to limit the flow, while political activists and others continue to push back against restrictions and find ways to circumvent censorship.

[8] Testimony of Nicole Wong, Google, op. cit. May 2, 2008.

[9] See Reporters Without Borders, "Handbook for Bloggers and Cyber-Dissidents," http://www.rsf.org/IMG/pdf/guide_gb_md-2.pdf.

[10] Prepared by Thomas Lum, Specialist in Asian Affairs, 7-7616.

[11] U.S. Department of State, 2008 *Human Rights Report: China*, February 25, 2009; PEN American Center, "Failing to Deliver: An Olympic-Year Report Card on Free Expression in China," July 8, 2008.

[12] Rebecca MacKinnon, "Bloggers and Censors: Chinese Media in the Internet Age," *China Studies Center*, May 18, 2007.

PRC officials have argued that Internet controls are necessary for social stability and that new restrictions target pornography and other "harmful content."[13] Chinese official commentary has suggested that the U.S. government has applied a double standard, regulating the Internet at home while calling for other countries to eliminate controls. The PRC government also has referred to U.S. criticism of Internet restrictions in China as politically motivated and an interference in China's domestic affairs.[14]

The PRC government employs a variety of methods to control online content and expression, including website blocking and keyword filtering; regulating and monitoring Internet service providers, Internet cafes, and university bulletin board systems; registering websites and blogs; and occasional arrests of high-profile "cyber dissidents" or crackdowns on Internet service providers.[15] Some analysts argue that even though the PRC government cannot control all Internet content and use, its selective targeting creates an undercurrent of fear and promotes self-censorship. Blocked websites, social networking sites, and file sharing sites include Radio Free Asia, international human rights websites, many Taiwanese newspapers, Facebook, Twitter, and YouTube. The government reportedly has hired thousands of students to express pro-government views on websites, bulletin boards, and chat rooms.[16] Furthermore, some analysts argue that the Internet has enhanced government propaganda and surveillance capabilities.

Nonetheless, the Internet has made it impossible for the Chinese government to restrict information as fully as before; bulletin boards, comment boards, chat rooms, blogs, and other outlets have allowed for an unprecedented amount of information and public comment on social and other issues. Although the state has the capability to block news of events or to partially shut down the Internet, as it did in Xinjiang following ethnic unrest that erupted there in July 2009, it often cannot do so before such events are publicized, if only fleetingly, online. The threat of public exposure or condemnation through the Internet reportedly has compelled some government officials to conduct affairs more openly. For Chinese Internet users in search of censored information, circumventing government controls is often made possible by way of "proxy servers" or "virtual private networks" using special software.[17] Furthermore, English language news sites, such as the *New York Times* and the *Washington Post*, are generally available.

U.S. Internet Companies, China, and Human Rights Issues

Some human rights activists and U.S. policy makers have expressed concern that U.S. Internet companies have sold Internet services or technologies to China that have assisted the PRC government in restricting information and communication and in monitoring and identifying Internet users. U.S. congressional committees and commissions have held hearings on the topics of global Internet freedom and the roles of U.S. Internet and technology companies in China's censorship regime. Some media watchdog groups and Members of Congress have maintained that some U.S. information technology companies, including Yahoo!, Microsoft, Google, and Cisco

[13] Kim Zetter, "China Stands Firm in Response to Google Threat," *Wired*, January 14, 2010.

[14] Gillian Wong, "China Denies Involvement in Google Hackings," *Associated Press*, January 25, 2010.

[15] Some experts estimate that the PRC government has employed 30,000 "Internet police." "On the Wrong Side of Great Firewall of China," *New Zealand Herald*, November 27, 2007.

[16] David Bandurski, "China's Guerrilla War for the Web," *Far Eastern Economic Review*, Vol. 171, no. 5 (July/August 2008).

[17] Such software is available internally and through foreign sources, including the U.S. government.

Systems, have provided willing, direct, sustained, or comprehensive support to PRC Internet censorship and political control efforts.[18]

U.S. information technology companies have responded that they must abide by the laws of the countries in which they operate, and that they are not actively cooperating or collaborating with the PRC government or tailoring their products to suit PRC censorship requirements.[19] These companies add that despite PRC censorship policies, they nonetheless are enlarging the volume of information available in China and other Internet-restricting countries, and can better press for freedom of expression and protection of privacy while located in these countries. They also claim that Chinese and other Asian and European competitors would fill the void in providing Internet services and technology in their absence. Furthermore, some Chinese experts have suggested that overall, the Internet, including foreign involvement, has created greater political freedom, despite the ongoing battle against growing PRC government attempts to control it.[20]

Yahoo!

Yahoo! has been blamed for complicity in the arrests of at least four Chinese Internet users by providing their e-mail account information to PRC authorities. In the most high-profile case, in 2004, Yahoo!'s Hong Kong office was accused of having provided information about the identity of a Chinese journalist and Yahoo! e-mail account holder, Shi Tao. Shi reportedly had forwarded information about state policy regarding the 15th anniversary of the Tiananmen demonstrations via his Yahoo! e-mail account to an overseas democracy group.[21] In March 2005, a PRC court sentenced Shi to 10 years in prison for "leaking state secrets." In August 2005, Yahoo! bought a 39% stake in China's Alibaba Group, a Chinese Internet service provider, and turned over its PRC operations to the Chinese company.

Microsoft

In 2005, Microsoft shut down the MSN Spaces site of Chinese political blogger Zhao Jing (a.k.a. Michael Anti) at the request of the PRC government, after Zhao had expressed support in his blog for a boycott of *Beijing News* following the firing of one of its editors. Human rights activists also criticized Microsoft for blocking words such as "democracy" from MSN Spaces. Microsoft was

[18] The Tom Lantos Human Rights Commission, "The State of Global Internet Freedom," June 18, 2009; U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Human Rights and the Law, *Global Internet Freedom: Corporate Responsibility and the Rule of Law*, May 20, 2008. U.S. Congress, House Committee on International Relations, Subcommittee on Africa, Global Human Rights and International Operations and Subcommittee on Asia and the Pacific, *The Internet in China: A Tool For Freedom or Suppression?*, February 15, 2006.

[19] Cisco's general counsel argued that Cisco does not customize its equipment for China; filtering technologies that are intrinsic to Cisco products cannot feasibly be eliminated; Cisco has a written code of conduct that aims to prevent the modification of its products in foreign countries in such as way as to undermine human rights; and Cisco complies with all U.S. government regulations or export controls that restrict the sale of high tech products and crime detection equipment. See Anne Broache, "Senators Weigh New Laws over China Online Censorship," news.cnet.com, May 20, 2008; Mark Chandler, Cisco Systems, Testimony before the Senate Committee on the Judiciary, Subcommittee on Human Rights and the Law, May 20, 2008; Mark Chandler, Cisco Systems, Testimony before the Subcommittee on Africa, Global Human Rights and International Operations and the Subcommittee on Asia and the Pacific of the Committee on International Relations, February 15, 2006.

[20] "Isaac Mao and Michael Anti at Hong Kong U.," April 17, 2007, http://rconversation.blogs.com/rconversation/2007/04/isaac_mao_and_m.html.

[21] Peter S. Goodman, "Yahoo Says it gave China Internet Data," *Washington Post*, September 11, 2005.

China's leading blog service provider at the time and remains one of the most popular. Recently, Microsoft also has been accused of cooperating with China's censorship policies in the development of its new *Bing* search engine.[22]

Google

Google's activities in China have reflected an attempt by the company to comply with PRC policies while limiting the company's role in censorship. Google's Chinese search engine, Google.cn, reportedly is the second-most widely used information-gathering service in China after that of *Baidu*, a Chinese company, and is the least censored, according to one study.[23] Google.cn provides a message stating that a website is unavailable due to "local laws, regulations, and policies," suggesting to the user that additional information exists, but that the government has closed access to that site. In 2006, Google reportedly moved its search records outside of the PRC in order to prevent the government from accessing the data without the company's consent, and does not host Gmail and Blogger services in China as a measure to protect the privacy of Chinese account holders.[24]

Ever since it entered the China market in 2005, Google and the PRC government have clashed over censorship and other issues, although the company has complied with Chinese laws in principle. In June 2009, China's Foreign Ministry accused the Internet company of violating PRC law and enabling Chinese Internet users to access "vulgar content." Google's Chinese service was disrupted for a few days, which some analysts viewed as the Chinese government response to Google's apparent resistance to abide by new censorship edicts.[25] Chinese writers accused Google of copyright infringement after the company began publishing their works in its online library, Google Books.[26] In October 2009, the *People's Daily*, the state's premier newspaper, accused Google of blocking its stories of the dispute.

Cisco Systems

Cicso Systems, Juniper Networks, Nortel of Canada, and Alcatel of France reportedly were involved in upgrading China's Internet infrastructure, filtering, and surveillance systems earlier this decade. According to some reports, Cisco Systems sold several thousand routers to China, which helped to facilitate the PRC government's censorship of Internet content and monitoring of Internet users.[27] According to other reports, Cisco sold technology to China's police force that can

[22] Christine Chiao, "Microsoft Erases Anti-Blog," *AsiaMedia*, January 17, 2006.

[23] Google's Chinese service, with roughly 80 million customers and 30 million Gmail accounts, has captured 20%-30% of the PRC market, compared to *Baidu*, which has over 60%. Tom Krazit, "Google's Censorship Struggles Continue in China," *news.cnet.com*, June 16, 2009; Steven Mufson, "China Faces Backlash from 'Netizens' if Google Leaves," *Washington Post*, January 13, 2010.

[24] Robert McMillan, "Google Moving Search Records Out of China," *InfoWorld*, March 1, 2006; Rory Cellan-Jones, "China and Google: What's Going On," *BBC – Dot.Life*, June 25, 2009; James Mulvenon, "The Rule of Law in China: Incremental Progress," *The China Balance Sheet in 2007 and Beyond*, Center for Strategic and International Studies, May 2007.

[25] Claudine Beaumont, "China Accuses Google of Spreading 'Vulgar Content,'" *Telegraph.co.uk*, June 25, 2009.

[26] "Google Apologizes to Chinese Writers," *Agence France Presse*, January 11, 2010.

[27] Jonathan Mirsky, "China's Tyranny Has the Best Hi-Tech Help Censoring the Internet," *International Herald Tribune*, January 16, 2006.

be used in the collection and use of data regarding personal background and imaging information, Web browsing history, and e-mail.[28]

The Continuing Battle Between Censorship and Freedom of Information

The PRC government has displayed a growing nervousness about the Internet's influence on Chinese society and politics, but it has been reluctant to provoke the ire of China's online population or to reduce the attractiveness of China's business environment for foreign investors. In June 2009, the PRC government issued a directive requiring "Green Dam Youth Escort" software, designed to prevent children from accessing "harmful content," such as pornography, on all Chinese computers sold after July 1, 2009, including those imported from abroad. Many Chinese Internet users, international human rights activists, foreign governments, chambers of commerce, and information technology manufacturers openly opposed the policy, arguing that the software would undermine computer operability, that it could be used to expand censorship to include political content, and that it could incorporate pirated software and weaken Internet security.[29] On June 30, 2009, the PRC government announced that mandatory installation of the software would be delayed for an indefinite period. On August 14, 2009, Minister of Industry and Information Technology Li Yizhong stated that the directive had created misunderstandings and that, "We will listen to the public's views before issuing a new directive on Green Dam."[30]

Following the aborted launch of "Green Dam," the PRC government has continued to tighten controls over Internet content and use, but in a quieter manner. In September 2009, PRC authorities issued requirements that new users register their true identities. This regulation reportedly has not been well enforced; however, the government can still track down individuals through their IP addresses. In December 2009, new restrictions aimed at cracking down on pornography, media piracy, and threats to national security and stability resulted in the closing of hundreds of websites, many of them entertainment-oriented. Furthermore, the China Internet Network Information Center announced that individuals could no longer apply for ".cn" domain names (China's country code), which it would now limit to registered business enterprises. Some observers argued that these policies could dampen the richness and vibrancy of Internet content and activity in China, as well as provoke a public backlash.[31] On October 15, 2009 (Internet Human Rights Day), 15 Chinese intellectuals issued a Declaration of Internet Human Rights calling for freedom of opinion, speech, and publication online.[32]

Google and Cyber Attacks

In January 2010, Google threatened to cease censoring its Chinese search engine or to pull out of China. The company asserted that, in December 2009, Chinese hackers had attacked its Gmail

[28] Steven Mufson, "China Turning to Technology to Hold onto Power," *Washington Post*, April 16, 2006; U.S. Congress, "The Internet in China: A Tool for Freedom or Suppression?" op. cit.

[29] In January 2010, a U.S. software firm filed a lawsuit against the Chinese government for copyright infringement, unfair competition, and other legal violations in connection with the Green Dam program. Agence France-Presse, "U.S. Software Firm Sues Chinese Government for US$2.2 Billion," *South China Morning Post*, January 6, 2010.

[30] "Green Dam Launch 'Not Handled Well'," http://www.chinaview.cn, August 14, 2009.

[31] Rebecca MacKinnon, "China Tightens Internet Controls in the Name of Fighting Porn, Piracy, and Cybercrime," *Rconversation* , December 14, 2009, http://rconversation.blogs.com; Sharon LaFraniere, "China Imposes New Internet Controls," *New York Times*, December 18, 2009.

[32] *Rconversation*, October 10, 2009, http://rconversation.blogs.com/rconversation/china/index.html.

service and corporate network as well as the computer systems of many other large U.S. corporations in the PRC.[33] Hackers appeared to have targeted the Gmail accounts of Chinese human rights activists; the intellectual property, including "source codes" or programming languages, of Google and other companies; and information on U.S. weapons systems. In a statement, Google's chief legal officer announced that the company would no longer censor results on Google.cn, even if that meant having to shut down the search engine, and potentially its offices in China.[34] Yahoo!, which was also hit by Chinese hackers, expressed support for Google's actions, thereby provoking an angry response by its PRC partner, *Alibaba*.

Chinese discussion boards and micro-blog postings indicated that a small majority of China's online population—and perhaps a large majority of its most active Internet users—wanted Google to stay in China, with some supporting Google's challenge to the PRC government. A significant minority adopted a pro-government stance or interpreted Google's move as profit-oriented.[35] According to some analysts, although China has huge potential, the company currently earns an estimated $300 million to $400 million from its China operations, a "tiny fraction" of its $22 billion in sales worldwide.[36]

While visiting Shanghai during his state visit to China in November 2009, President Barack Obama expressed support of unrestricted Internet access and disapproval of censorship. On January 21, 2010, in a policy speech on Internet freedom, Secretary of State Hillary Clinton urged U.S. Internet companies to oppose censorship in their overseas operations and announced that the Global Internet Freedom Taskforce (GIFT) would be reinvigorated. She also called upon the PRC government to conduct a thorough investigation of the December 2009 cyberattacks upon U.S. companies in China and to make its results transparent. Beijing denied involvement in the attacks and defended its Internet policies. The Foreign Ministry stated that foreign companies, including Google, "should respect the laws and regulations, respect the public interest of Chinese people and China's culture and customs and shoulder due social responsibilities."[37]

Iran[38]

The Iranian government has restricted Internet usage since access spread beyond universities and government agencies to the general population in the late 1990s. Today, Iran has an estimated 23 million Internet users,[39] and watchdog groups and Internet activists claim that Iran's filtering and

[33] Estimates of the number of U.S. information technology, finance, defense, and other companies targeted in this attack ranged from 20 to 34.

[34] Google representatives stated that two Gmail accounts appeared to have been accessed but that the content of e-mail communications had not been breached. "Statement from Google: A New Approach to China," *Washington Post*, January 12, 2010. See also "A New Approach to China," *The Official Google Blog*, January 12, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

[35] Jessica E. Vascellaro and Aaron Back, "Fallout from Cyber Attack Spreads—Google Investigates China Employees; Rift Emerges Between Yahoo! and Alibaba," *Wall Street Journal*, January 19, 2010; Rebecca MacKinnon, "Google Puts Its Foot Down," *RConversation*, http://rconversation.blogs.com/rconversation/china/index.html, January 13, 2010.

[36] Miguel Helft, "For Google, A Threat to China with Little Revenue at Stake," *New York Times*, January 15, 2010.

[37] "Clinton Urges Global Internet Freedom," *VOA News.com*, January 21, 2010; Gillian Wong, "China Denies Involvement in Google Hackings," *Washington Post*, January 25, 2010; "China Says Google 'No Exception to Law'," Embassy of the People's Republic of China in the United States, January 19, 2010.

[38] Prepared by Casey Addis, Analyst in Middle Eastern Affairs, 7-0846.

[39] "ITU Internet Indicators 2008," International Telecommunications Union, http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&RP_intYear=2008& (continued...)

monitoring of usage is among the most extensive in the world. Additional information about Iran's Internet policies is available from the U.S. Department of State in its annual report, *2008 Country Reports on Human Rights Practices*.

The Iranian government tracks online communication and content through a centralized location in the state's telecommunications monopoly, the Ministry of Communications and Information Technology (MCIT). In addition to its 23 million Internet users, the Persian blogosphere is among the world's most robust. The status of Internet sites and blogs remains contested under Iranian law, but the Press Law does require that bloggers obtain licenses, and all content on websites and blogs is subject to approval of the Ministry of Culture and Islamic Guidance (MCIG). The government also regulates access to the Internet by limiting the speed of Internet access that ISPs can provide to households and public access sites (Internet cafes) to 128 kilobytes per second, making it difficult or impossible to download multimedia content. Iran reportedly is the only country to have imposed a cap on Internet access speed for households.[40] Iran also has arrested numerous activists, bloggers, and journalists on charges of "antigovernment publicity," "propaganda against the Islamic Republic," and "jeopardizing national security."[41]

The government has disabled the Internet altogether in the past, usually during elections, but some observers argue that improvements in monitoring and filtering technologies have made such measures unnecessary and even enabled the government to use the Internet to disseminate disinformation and pro-government content. Following the disputed 2009 presidential election, the Internet was reportedly slow but accessible. The number of detentions of Internet activists and bloggers increased during the post-election unrest, arguably demonstrating the extent of government filtering and monitoring of usage. The post-election crackdown on Internet freedom raised concerns that Iran's human rights abuses were being aided by Western technology companies. Others said the concerns were being overstated, asserting that Iran also develops its own filtering and monitoring technologies.

The Nokia Siemens Network (NSN)[42] sold communication monitoring equipment to the Iranian government in 2008.[43] The monitoring center, installed into the MCIT gateway, was part of a larger contract with Iran that included mobile phone network technology. The Iranian government had reportedly experimented with the monitoring equipment prior to the election, but did not use it extensively until after the election. Some experts have argued that the nature of the content inspection happening in Iran since the election goes beyond the practices of other countries, including China.[44]

(...continued)

RP_intLanguageID=1.

[40] "Speed Reduced for High Speed Internet in Iran," *BBC Persian*, October 20, 2006.

[41] See the U.S. State Department "2008 Human Rights Report: Iran," http://www.state.gov/g/drl/rls/hrrpt/2008/nea/119115.htm.

[42] NSN is a joint venture between the Finnish cell phone maker Nokia and the German company Siemens.

[43] Stuart Smith, "Politics of Marketing: Why Brands Continue to Surf the Recession," *Marketing Week* (London), August 13, 2009.

[44] See Christopher Rhoads and Loretta Chao, "Iran's Web Spying Aided by Western Technology," *Wall Street Journal*, June 22, 2009.

NSN maintains that it sold the technology for the purpose of "lawful intercept" of information used to track criminals and terrorists.[45] Critics argue that in a country like Iran, where the population is heavily reliant on Internet communication with the outside world due to censorship of other communication, this technology enables the government to intensify repression.[46]

U.S. Law and Internet Freedom Abroad[47]

In response to laws and regulations of foreign countries requiring censorship and disclosure of users' personal information, some U.S. technology firms engage in Internet censoring and filtering. Some examples include China and other Internet-restricting countries such as Iran. In some cases, such as in Iran, Internet censoring and filtering reportedly involve a practice often called deep packet inspection which is under a great deal of scrutiny in the United States.[48] Doing business in a foreign country subjects the business to the jurisdiction of that country.[49] Nonetheless, concerns have been raised that China's Internet filtering could run afoul of world trade obligations.[50]

U.S. Policy for the Promotion of Internet Freedom Abroad[51]

The importance of Internet freedom to the United States was declared in 2006. During an explanation of that year's State Department 2006 *Country Reports on Human Rights Practices*, then-Under Secretary of State for Democracy and Global Affairs Paula J. Dobriansky explained that the 2006 reports included new, additional focus on "the extent to which internet access is available to and used by citizens in each country and ... whether governments inappropriately limit or block access to the internet or censor websites."[52] This was added as an area of concern because the internet is playing a growing role in people's ability to freely express themselves and in the free flow of information. In discussing this new area of focus, then-Under Secretary Dobriansky said,

> We will continue to defend internet freedom, including by addressing internet repression directly with the foreign governments involved and seeking to persuade foreign officials that

[45] Nokia Siemens Networks, "Provision of Lawful Intercept Capability in Iran," June 22, 2009, http://www.nokiasiemensnetworks.com/press/press-releases/provision-lawful-intercept-capability-iran.

[46] Eli Lake, "Fed Contractor, Cell Phone Maker Sold Spy System to Iran," *Washington Times*, April 13, 2009.

[47] Prepared by Gina Stevens, Legislative Attorney, 7-2581.

[48] Deep Packet Inspection ("DPI") is a computer network packet filtering technique that involves the inspection of the contents of data packets as they are transmitted across the network.

[49] Many foreign countries have privacy laws that may be applicable to Internet Service Providers, websites, etc. See Morrison & Foerster's Privacy Library for the text of privacy laws in other countries, in the U.S., and for multinational organizations, http://www.mofoprivacy.com/default.aspx?tabNum=2.

[50] See Andrew Noyes, "Chinese Demands for Web Filtering Software Cause a Stir," *CongressDailyAM*, June 25, 2009; Tim Wu, "The World Trade Law of Censorship and Internet Filtering," *Chi. J. Int'l L.*, vol. 7 (2006-07).

[51] Prepared by Kennon H. Nakamura, Analyst in Foreign Affairs, 7-9514.

[52] Under Secretary of State for Democracy and Global Affairs Paula Dobriansky, "On-The-Record Briefing on the State Department's *2006 Country Reports on Human Rights Practices*," Washington, March 6, 2007, http://www.state.gov/g/drl/rls/rm/2007/81468.htm.

> restricting internet freedom is contrary to their own interests and that of their countries. The new information in this year's reports will make an important contribution.[53]

At this same time, then-Secretary of State Condoleezza Rice also established the Global Internet Freedom Task Force (GIFT) in order to provide a U.S. foreign policy response to violations of Internet freedom by repressive regimes around the world.[54]

Secretary of State Hillary Rodham Clinton, in a January 21, 2010, speech, stated that Internet freedom is a central part of U.S. foreign policy. She stated that Internet freedom is more than a question of information freedom, it is about the nature of the world we want to inhabit. Clinton further stated: "It's about whether we live on a planet with one Internet, one global community, and a common body of knowledge that benefits and unites us all, or a fragmented planet in which access to information and opportunity is dependent on where you live and the whims of censors."[55]

In her remarks, Secretary Clinton placed the United States on the side of a single Internet where everyone has equal access to knowledge and ideas. She noted that blogs, e-mails, social networks, and text messages are opening up a new virtual town square where citizens can go to criticize their governments and exchange ideas. U.S. responsibility to support this new "town square" is not new but can be found in the First Amendment of the U.S. Bill of Rights ensuring freedom of speech, assembly, and religion. Secretary Clinton argued that these principles were reaffirmed in President Franklin Roosevelt's "The Four Freedoms" speech,[56] and in the work of the United States and its support of the Universal Declaration of Human Rights.

Secretary Clinton further explained that U.S. foreign policy is premised on the idea that no country stands to benefit more than the United States when there is cooperation among peoples and states. No country shoulders a heavier burden than the United States when conflict and misunderstanding make the international system unstable, and force people and countries apart. She stated that it is important that the United States seizes the opportunities that come with interconnectivity and work for a world in which access to networks and information brings people closer together and expands the definition of the global community.

Secretary Clinton continued the GIFT and its responsibilities. The Task Force is co-chaired by the Under Secretaries of State for Democracy and Global Affairs and for Economic, Business, and Agricultural Affairs and draws on the State Department's multidisciplinary expertise in its regional and functional bureaus to work on issues such as international communications, human rights, democratization, business advocacy and corporate social responsibility, and country specific concerns. The task force supports Internet freedom by[57]

---

[53] Ibid.

[54] U.S. Mission to the United Nations in Geneva, "Secretary of State Establishes New Global Internet Freedom Task Force," press release, February 14, 2006, http://geneva.usmission.gov/Press2006/02141InternetTaskForce.html.

[55] Secretary of State Hillary Rodham Clinton, "Remarks on Internet Freedom," January 21, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm.

[56] On January 6, 1941, President Franklin Roosevelt addressed Congress saying that "we look forward to a world founded upon four essential human freedoms." These essential freedoms, which he referred to as the "Four Freedoms" are (1) freedom or speech and expression, (2) freedom of religion, (3) freedom from want, and (4) freedom from fear.

[57] The GIFT Strategy is available online at http://2001-2009.state.gov/g/drl/rls/78340.htm.

- monitoring Internet freedom and reporting in its annual *Country Reports on Human Rights Practices* the quality of Internet freedom in each country around the world;
- responding in both bilateral and international fora to support Internet freedom; and
- expanding access to the Internet with greater technical and financial support for increasing availability of the Internet in the developing world.

In advancing Internet freedom as an objective of U.S. foreign policy, Secretary Clinton proposed a number of key initiatives:[58]

- Continue the work of the State Department's GIFT as it oversees U.S. efforts in more than 40 countries to help individuals circumvent politically motivated censorship by developing new tools and providing the training needed to safely access the Internet;
- Make Internet freedom an issue at the United Nations and the U.N. Human Rights Council in order to enlist world opinion and support for Internet Freedom;
- Work with new partners in industry, academia, and non-governmental organizations to establish a standing effort to advance the power of "connection technologies" that will empower citizens and leverage U.S. traditional diplomacy;
- Provide new, competitive grants for ideas and applications that help break down communications barriers, overcome illiteracy, and connect people to servers and information they need;
- Urge and work with U.S. media companies to take a proactive role in challenging foreign governments' demands for censorship and surveillance; and
- Encourage the voluntary work of the communications-oriented, private sector-led Global Network Initiative (GNI). The GNI brings technology companies, nongovernmental organizations, academic experts, and social investment funds together to develop responses and mechanisms to government requests for censorship.

To fund U.S. efforts in support of Internet freedom, Congress in FY2008 appropriated $15 million, most of which has been spent or is obligated. Another $5 million was appropriated in FY2009. Finally, in Secretary Clinton's January 21 speech, she spoke of an additional $15 million for FY2010 that has been allocated from State Department appropriations to a range of programs that, in full or in part, support Internet freedom. Assistant Secretary for Democracy, Human Rights, and Labor Michael Posner describes these programs as "not just circumvention…. [I]t's a lot about training people…. It's some about technology. It's some about encouraging groups that are in danger. It's a lot about diplomacy, too, for us getting out there and being sure that when groups are in trouble, we provide a lifeline."[59]

[58] Hillary Rodham Clinton, "Remarks on Internet Freedom," op. cit.

[59] Assistant Secretary of State for Democracy, Human Rights, and Labor Michael H. Posner, "Briefing on Internet Freedom and 21st Century Statecraft," January 22, 2010, http://www.state.gov/g/drl/rls/rm/2010/134306.htm.

The U.S. Broadcasting Board of Governors' International Broadcasting Bureau also supports counter-censorship technologies and has committed approximately $2 million per year to help enable Internet users in repressive regimes to have access to the VOA and other U.S. governmental and non-governmental websites and to receive VOA e-mail newsletters.

Some observers have expressed concerns that there could be serious negative consequences for U.S. and foreign companies, and U.S. or foreign nationals working or living in countries with repressive regimes, if they follow the expanded U.S. policy supporting Internet freedom. These commenters point out that repressive governments could punish or make an example of an individual or company for not following the dictates of that country. Such actions could include harassment, lifting of business licenses, confiscation of assets, or imprisonment. These observers question what powers, beyond expressing U.S. displeasure through official demarches and public statements or through negotiations, that the United States may have to respond to such actions.[60]

Congressional Action

In 2010, Congress has taken steps to address ongoing concerns about ensuring the free and secure flow of information over the Internet:

- On March 10, 2010, the House Committee on Foreign Affairs conducted a hearing, "The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade," on the December 2009 Chinese cyber attacks on Google and other U.S. companies, to consider policy tools to address Internet freedom, trade, and cyber security issues;
- On March 9, 2010, Representatives David Wu and Christopher Smith announced the formation of the House Global Internet Freedom Caucus; and
- The Senate Judiciary Committee, Subcommittee on Human Rights and the Law, held a hearing on March 2, 2010, entitled "Global Internet Freedom and the Rule of Law, Part II" to examine human rights, corporate responsibility, and other issues related to Internet censorship around the world.

The Global Network Initiative: Private Sector Support of Internet Freedom[61]

The Global Network Initiative (GNI) was formed in October 2008 to respond to criticism of Internet service providers and computer manufacturers who had sold technology or services to Internet-restricting countries.[62] GNI was launched by a coalition of human rights organizations, academics, investors and technology leaders. GNI adopts a self-regulatory approach to protect and advance individuals' rights to free expression and privacy on the Internet. A set of principles

[60] Questions following Secretary of State Hillary Clinton's *Remarks on Internet Freedom*, January 21, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm, and questions following Assistant Secretary of State Michael Posner's "Briefing on Internet Freedom and 21st Century Statecraft," January 22, 2010, http://it.tmcnet.com/news/2010/01/26/4590599.htm.

[61] Originally prepared by Gina Stevens, Legislative Attorney, 7-2581.

[62] See http://www.globalnetworkinitiative.org/.

and supporting mechanisms provide guidance to the information and communications technology (ICT) industry and its stakeholders on how to protect and advance the human rights of freedom of expression and privacy when faced with pressures from governments to take actions that infringe upon these rights.

Governments are not members of the GNI, but are encouraged to support the principles and encourage their adoption. Organizations participating in the GNI include Google Inc., Microsoft Corp., and Yahoo! Inc. Each initial participating company committed $100,000 per year over the two-year start-up period. Organizations not participating in the initiative who where involved in its development include Amnesty International and Reporters Without Borders. Reporters Without Borders remains skeptical about how much change GNI can effect, and pushed for standards that would require all government requests and takedown notices be made in writing.

The GNI's Principles on Freedom of Expression and Privacy ("the Principles") are based on internationally recognized laws and standards for human rights, including the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights.

The GNI acknowledges that the rights of privacy and of freedom of expression should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws or standards. The Implementation Guidelines ("The Guidelines") of the GNI provide guidance to ICT companies on how to implement the Principles, and describe the actions that constitute compliance.

With respect to government demands to remove or limit access to content or restrict communications, participating companies commit to encourage governments to

- be specific, transparent, and consistent in the demands issued to restrict freedom of expression online;
- encourage government demands that are consistent with international laws and standards;
- require governments to follow local legal processes, interpret government demands so as to minimize the negative effect, when required to restrict communications or remove content; and
- interpret the governmental authority's jurisdiction to minimize the negative effect.

Participating companies commit to operate in a transparent manner when required to remove content or restrict access, and must disclose to users the applicable laws and policies requiring such action, the company's policies for responding to government demands, and provide timely notice to users when access to content has been locked or communications limited due to government restrictions. With respect to privacy, participating companies commit to assess the human rights risks associated with the collection, storage, and retention of personal information and to develop mitigation strategies.

A system of independent third-party assessment of company compliance with the Principles and Implementation Guidelines will be phased in over three stages:

- In Phase One (ends December 2010) each participating company establishes internal policies and procedures to implement the Principles, and the Board approves independence and competence criteria for the selection of independent assessors.
- In Phase Two (2011) independent assessors will conduct process assessments of each participating company to review and evaluate their internal systems for implementing the Principles.
- In Phase Three (January 2012 onwards) the Board will accredit independent assessors to review the internal systems of companies, and company responses to specific government demands implicating freedom of expression or privacy. Each participating company will submit an annual report to the Organization. The assessors will prepare reports explaining each company's responses to government demands, evaluating the effectiveness of the company's responses. Each company will be given the opportunity to respond to the assessor's draft and final report. The Board of the Organization will assess whether the company is in compliance with the Principles and its determination will be made public. The Board of the Organization will publish an annual report assessing each participating company's compliance with the Principles.

Recent Legislative Action[63]

Public Laws

H.R. 2647, *National Defense Authorization Act for Fiscal Year 2010*. Introduced by Representative Skelton (by request), referred to the House Armed Services Committee. Enacted October 28, 2009, P.L. 111-84.

Title XII: Matters Relating to Foreign Nations

Subtitle D: VOICE Act - Victims of Iranian Censorship Act or VOICE Act

(Sec. 1242) Expresses the sense of the Senate in support of the universal values of freedom of speech, the press, and expression as it pertains to the people of Iran, and condemns acts of censorship, intimidation, and other restrictions on such freedom in Iran.

(Sec. 1243) States that it shall be the policy of the United States to (1) support freedom of the press, speech, expression, and assembly in Iran; (2) support the Iranian people as they seek, receive, and impart information and promote ideas in writing, print, and through other media; (3) discourage businesses from aiding efforts to interfere with the ability of the Iranian people to access or share information or otherwise infringe upon such freedoms; and (4) encourage the development of technologies that facilitate efforts of the Iranian people to share such information, exercise such freedoms, and engage in Internet-based education programs and other exchanges between U.S. citizens and Iranians.

[63] Legislative summaries are taken directly from the Legislative Information Service of the Library of Congress.

(Sec. 1244) Authorizes appropriations for the (1) International Broadcasting Operations Fund to expand Farsi language programming and to disseminate accurate and independent information to the Iranian people through radio, television, Internet, cellular telephone, short message service, and other communications; and (2) Broadcasting Capital Improvements Fund to expand transmissions of Farsi language programs to Iran.

(Sec. 1245) Establishes in the Treasury the Iranian Electronic Education, Exchange, and Media Fund to support the development of technologies that will aid the Iranian people in exchanging information and exercising freedom of speech, expression, and assembly. Authorizes appropriations to the Fund.

(Sec. 1246) Directs the President to report annually to Congress on the use of funds authorized under this Subtitle.

(Sec. 1247) Requires the President to (1) direct the appropriate officials to examine claims that non-Iranian companies have provided hardware, software, or other forms of assistance to the government of Iran that has furthered its efforts to filter online political content, disrupt cell phone and Internet communications, and monitor the online activities of Iranian citizens; and (2) report study results to Congress.

(Sec. 1248) Authorizes appropriations to the Secretary of State to document, collect, and disseminate information about human rights in Iran, including abuses since the Iranian presidential election on June 12, 2009.

Bills and Resolutions in the House of Representatives

H.R. 2271, *Global Online Freedom Act of 2009*. Introduced by Representative Christopher Smith and referred to the House Committee on Foreign Affairs; and the House Committee on Energy and Commerce.

Makes it U.S. policy to (1) promote the freedom to seek, receive, and impart information and ideas through any media; (2) use all appropriate instruments of U.S. influence to support the free flow of information without interference or discrimination; and (3) deter U.S. businesses from cooperating with Internet-restricting countries in effecting online censorship.

Expresses the sense of Congress that (1) the President should seek international agreements to protect Internet freedom; and (2) some U.S. businesses, in assisting foreign governments to restrict online access to U.S.-supported websites and government reports and to identify individual Internet users, are working contrary to U.S. foreign policy interests.

Amends the Foreign Assistance Act of 1961 to require assessments of electronic information freedom in each foreign country.

Establishes in the Department of State the Office of Global Internet Freedom (OGIF).

Directs the Secretary of State to annually designate Internet-restricting countries. Prohibits, subject to waiver, U.S. businesses that provide to the public a commercial Internet search engine, communications services, or hosting services from locating, in such countries, any personally identifiable information used to establish or maintain an Internet services account.

Requires U.S. businesses that collect or obtain personally identifiable information through the Internet to notify the OGIF and the Attorney General before responding to a disclosure request from an Internet-restricting country. Authorizes the Attorney General to prohibit a business from complying with the request, except for legitimate foreign law enforcement purposes.

Requires U.S. businesses to report to the OGIF certain Internet censorship information involving Internet-restricting countries.

Prohibits U.S. businesses that maintain Internet content hosting services from jamming U.S.-supported websites or U.S.-supported content in Internet-restricting countries.

Authorizes the President to waive provisions of this act: (1) to further the purposes of this act; (2) if a country ceases restrictive activity; or (3) if it is the national interest of the United States.

H.R. 4784,[64] *Internet Freedom Act of 2010.* Introduced by Representative Wu and referred to the House Science and Technology Committee, Subcommittee on Research and Science Education.

Directs the National Science Foundation to establish the Internet Freedom Foundation governed by a board of 12 members, with equal representation from government, academia, and the private sector. The Internet Freedom Foundation shall—

- Award competitive, merit-reviewed grants, cooperative agreements, or contracts to private industry, universities, and other research and development organizations to develop deployable technologies to defeat Internet suppression and censorship; and
- Award incentive prizes to private industry, universities, and other research and development organizations that successfully develop deployable technologies to defeat Internet suppression and censorship.

The Internet Freedom Foundation shall be funded by such sums as may be necessary.

H.Res. 590, *Expressing grave concerns about the sweeping censorship, privacy, and cybersecurity implications of China's Green Dam filtering software, and urging U.S. high-tech companies to promote the Internet as a tool for transparency, freedom of expression, and citizen empowerment around the world.* Introduced by Representative Wu and referred to the House Committee on Foreign Affairs.

Expresses (1) grave concerns about the sweeping censorship, privacy, and cybersecurity implications of China's Green Dam filtering software; and (2) support for the Chinese people in their quest for Internet freedom and free expression.

Calls on (1) the Chinese government to rescind its requirement for Green Dam to be preinstalled on all new computers; and (2) U.S. high-tech companies to promote the Internet as a tool for transparency, freedom of expression, and citizen empowerment around the world.

[64] This bill is a substitute for H.R. 4595.

H.Res. 672, *Calling on the Government of the Socialist Republic of Vietnam to release imprisoned bloggers and respect Internet freedom*. Introduced by Representative Sanchez and referred to the House Committee on Foreign Affairs. Passed on October 21, 2009.

Supports the right of the citizens of the Socialist Republic of Vietnam to access websites of their choosing and to have the freedom to share and publish information over the Internet.

Calls on Vietnam to (1) repeal Circular 07, Article 88, and similar statutes that restrict the Internet, so as to be in line with the International Covenant on Civil and Political Rights, to which Vietnam is a signatory; (2) become a responsible member state of the international community by respecting individuals' freedom of speech, freedom of press, and freedom of political association; and (3) release all political prisoners, including but not limited to 18 named bloggers and cyber activists.

Appendix A. Technologies Used to Monitor and Censor Web Sites and Web-Based Communications[65]

Key-Word List Blocking

This is a simple type of filtration where a government drops any Internet packets featuring certain keywords, such as "protest" or "proxy."

Domain Name System (DNS) Poisoning

DNS poisoning intentionally introduces errors into the Internet's directory service to misdirect the original request to another IP address.

IP Blocking

IP Blocking is one of the most basic methods that governments use for censorship, as it simply prevents all packets going to or from targeted IP addresses. This is an easy technology to implement, but it does not address the problem of individual communications between users. This method is used to block banned websites, including news sites and proxy servers that would allow access to banned content, from being viewed.

Bandwidth Throttling

Bandwidth throttling simply limits the amount of traffic that can be sent over the Internet. Keeping data volume low facilitates other methods of monitoring and filtering by limiting the amount of data present.

Traffic Classification

This is a much more sophisticated method of blocking traffic than IP blocking, as governments can halt any file sent through a certain type of protocol, such as FTP. Because the government knows that FTP transfers are most often sent through TCP port 21, they can simply limit the bandwidth available on that port and throttle transfers. This type of traffic-shaping practice is the most common one used by repressive governments today. It is not resource intensive and it is fairly easy to implement.

Shallow Packet Inspection (SPI)

Shallow packet inspection is a less sophisticated version of the deep packet inspection (DPI) technique (DPI is described below) that is used to block packets based on their content. Unlike

[65] Prepared by Patricia Moloney Figliola, Specialist in Telecommunication and Internet Policy, 7-2508. Adapted from "The State of Iranian Communication: Manipulation and Circumvention," Morgan Sennhauser, Nedanet, July 2009, http://iranarchive.openmsl.net/SoIC-1.21.pdf; and "Five Technologies Iran is Using to Censor the Web," Brad Reed, Network World, July 2009, http://www.networkworld.com/news/2009/072009-iran-censorship-tools.html.

DPI, which intercepts packets and inspects their fingerprints (fingerprinting is described below), headers, and payloads, SPI makes broad generalities about traffic based solely on evaluating the packet header. Although shallow packet inspection can't provide the same refined/detailed traffic assessments as DPI, it is much better at handling volume than DPI.

SPI is much less refined than DPI, but it is capable of handling a greater volume of traffic much more quickly. SPI is akin to judging a book by its cover. This method is prone to exploitation by users because they can disguise their packets to look like a different kind of traffic.

Packet Fingerprinting

This is a slightly more refined method of throttling packets than shallow packet inspection, as it looks not only at the packet header but at its length, frequency of transmission, and other characteristics to make a rough determination of its content. In this manner, the government can better classify packets and not throttle traffic sent out by key businesses.

Deep Packet Inspection (DPI) / Packet Content Filtering

DPI is the most refined method that governments have for blocking Internet traffic. As mentioned above, deep packet inspectors examine not only a packet's header but also its payload. For instance, certain keywords can be both monitored and the e-mail containing them can be kept from reaching its intended destination.

This gives governments the ability to filter packets at a more surgical level than any of the other techniques discussed so far. While providing the most targeted traffic monitoring and shaping capabilities, DPI is also more complicated to run and is far more labor-intensive than other traffic-shaping technologies.

Appendix B. Technologies Used to Circumvent Censorship[66]

Each of the circumvention methods explained below can, in general, be considered an anonymous "proxy server." A proxy server is a computer system or an application program that acts as an intermediary for requests from a user seeking resources from other servers, allowing the user to block access to his or her identity and become anonymous.

Web-Based Circumvention Systems

Web-based circumvention systems are special web pages that allow users to submit a URL and have the web-based circumventor retrieve the requested web page. There is no connection between the user and the requested website as the circumventor transparently proxies the request allowing the user to browse blocked websites seamlessly. Since the web addresses of public circumventors are widely known, most Internet filtering applications already have these services on their block lists, as do many countries that filter at the national level.

Examples: Proxify, StupidCensorhip, CGIProxy, psiphon, Peacefire/Circumventor.

Web and Application Tunneling Software

Tunneling encapsulates one form of traffic inside of other forms of traffic. Typically, insecure, unencrypted traffic is tunneled within an encrypted connection. The normal services on the user's computer are available, but run through the tunnel to the non-filtered computer which forwards the user's requests and their responses transparently. Users with contacts in a non-filtered country can set up private tunneling services while those without contacts can purchase commercial tunneling services. "Web" tunneling software restricts the tunneling to web traffic so that web browsers will function securely, but not other applications. "Application" tunneling software allows the user to tunnel multiple Internet applications, such as e-mail and instant messenger applications.

Examples: Web Tunneling: UltraReach, FreeGate, Anonymizer, Ghost Surf.
Examples: Application Tunneling: GPass, HTTP Tunnel, Relakks, Guardster/SSH.

Anonymous Communications Systems

Anonymous technologies conceal a user's IP address from the server hosting the website visited by the user. Some, but not all, anonymous technologies conceal the user's IP address from the anonymizing service itself and encrypt the traffic between the user and the service. Since users of anonymous technologies make requests for web content through a proxy service, instead of to the server hosting the content directly, anonymous technologies can be a useful way to bypass

[66] Adapted from *Reporters Without Borders*, "Handbook for Bloggers and Cyber-Dissidents," September 2005, http://www.rsf.org/IMG/pdf/Bloggers_Handbook2.pdf; and *The Citizen Lab*, "Everyone's Guide to By-Passing Internet Censorship for Citizens Worldwide," University of Toronto, September 2007, http://citizenlab.org/Circ_guide.pdf.

Internet censorship. However, some anonymous technologies require users to download software and can be easily blocked by authorities.

Examples: Tor, JAP ANON, I2P

Author Contact Information

Patricia Moloney Figliola, Coordinator
Specialist in Internet and Telecommunications Policy
pfigliola@crs.loc.gov, 7-2508

Casey L. Addis
Analyst in Middle Eastern Affairs
caddis@crs.loc.gov, 7-0846

Kennon H. Nakamura
Analyst in Foreign Affairs
knakamura@crs.loc.gov, 7-9514

Thomas Lum
Specialist in Asian Affairs
tlum@crs.loc.gov, 7-7616