

Promoting Global Internet Freedom: Policy and Technology

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

October 22, 2013

Congressional Research Service
7-5700
www.crs.gov
R41837

CRS Report for Congress
Prepared for Members and Committees of Congress

c11173008

Summary

Modern communication tools such as the Internet provide a relatively inexpensive, accessible, easy-entry means of sharing ideas, information, and pictures 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 social networking sites, as well as the blogs, video sharing sites, and other tools of today's communications technology, have 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.

Internet freedom can be promoted in two ways, through legislation that mandates or prohibits certain activities, or through industry self-regulation. Current legislation under consideration by Congress, the *Global Online Freedom Act of 2011* (H.R. 3605), would prohibit or require reporting of the sale of Internet technologies and provision of Internet services to "Internet-restricting countries" (as determined by the State Department). Some believe, however, that technology can offer a complementary and, in some cases, better and more easily implemented solution to ensuring Internet freedom. 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 about federal and private sector efforts to promote and support global Internet freedom and a description of Internet freedom legislation and hearings from the 113th and 112th Congresses. Three appendixes suggest further reading on this topic and describe censorship and circumvention technologies.

Contents

Introduction 1
Doing Business with Repressive Regimes: U.S. Industry Dilemma 1
U.S. Government Activity Promoting Internet Freedom 2
Department of State 2
The NetFreedom Task Force 3
Freedom Online Coalition 4
The State Department's International Strategy for Cyberspace 5
Broadcasting Board of Governors 6
U.S. Industry Activity Promoting Internet Freedom: The Global Network Initiative 6
GNI Report: Protecting Human Rights in the Digital Age 7
Legislative Activity in the 113th Congress 8
Legislation 8
Hearings 9
Legislative Activity in the 112th Congress 9
Legislation 9
Hearings 9

Appendixes

Appendix A. For Further Reading 10
Appendix B. Methods/Technologies Used to Monitor and Censor Websites and Web-Based Communications 11
Appendix C. Technologies Used to Circumvent Censorship 13

Contacts

Author Contact Information 14
Acknowledgments 14

Introduction

Around the world, over 2 billion people have access to the Internet. Most use this access to conduct activities related to their day-to-day lives—such as accessing government services, banking and paying bills, communicating with friends and relatives, researching health information, and, in some cases, participating in their counties' political processes. In most countries, those who use the Internet to participate in their countries' political processes take for granted that they may use the Internet to engage openly in political discussions and to organize politically-oriented activities.

However, the freedoms of speech, association, and assembly—including both political speech and organizing conducted via the Internet—are not available to citizens in every country. In some countries activists are in danger any time they access or even attempt to access a prohibited website or service or promote political dissent. Political activity is monitored and tracked. Despite such hurdles, political activists have embraced the Internet, using it to share information and organize dissent. To protect themselves, they have purchased and deployed circumvention technologies to skirt government censors.

The restriction of Internet freedom by foreign governments creates a tension between U.S. policy makers and industry. One of the most fundamental of these tensions is between the commercial needs of U.S. industry, which faces competitive and legal pressures in international markets, and the political interests of the United States, which faces other pressures (e.g., national security, global politics). This tension is complicated by the fact that many of the technologies in question may be used both for and against Internet freedom, in some cases simultaneously.

This report provides information about federal and private sector efforts to promote and support global Internet freedom, a description of Internet freedom legislation from the 113th and 112th Congresses, and suggestions for further reading on this topic. Two appendixes describe censorship and circumvention technologies.

Doing Business with Repressive Regimes: U.S. Industry Dilemma

Governments everywhere need the Internet for economic growth and technological development. Some also seek to restrict the Internet in order to maintain social, political, or economic control. Such regimes often require the assistance of foreign Internet companies operating in their countries. These global technology companies find themselves in a dilemma. They must either follow the laws and requests of the host country, or refuse to do so and risk the loss of business licenses or the ability to sell services in that country.

However, the global technology industry also risks raising the concern of U.S. lawmakers by appearing to be complicit with a repressive regime if they cooperate. For example, the Global Online Freedom Act of 2011 (GOFA) (H.R. 3605), introduced by Representative Christopher Smith, would prohibit or require reporting of the sale of Internet technologies and provision of Internet services to "Internet-restricting countries" (as determined by the State Department). That legislation mirrors opinions of some who believe that the U.S. technology industry should be doing more to ensure that its products are not used for repressive purposes.

Others believe that technology can offer a complementary (and, in some cases, better) solution to prevent government censorship than mandates imposed on companies. Hardware, software, and Internet services, in and of themselves, are neutral elements of the Internet; it is how they are implemented by various countries that makes them "repressive." For example, software is needed by Internet service providers (ISPs) to provide that service. However, software features intended for day-to-day Internet traffic management, such as filtering programs that catch spam or viruses, can be misused. Repressive governments use such programs to censor and monitor Internet traffic—sometimes using them to identify specific individuals for persecution. Further, U.S. technology representatives note that it is not currently feasible to completely remove these programs, even when sold to countries that use those features to repress political speech, without risking significant network disruptions.[1]

On the other hand, widely used Internet services, such as search engines, are often tailored for 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.[2]

U.S. Government Activity Promoting Internet Freedom

Both the Department of State and the Broadcasting Board of Governors (BBG) have an active role in fighting Internet censorship.

Department of State

The State Department works to "protect and defend a free and open Internet"[3] as an element of its policy supporting universal rights of freedom of expression and the free flow of information. It supports the following key initiatives to advance Internet freedom as an objective of U.S. foreign policy:[4]

- Continue the work of the State Department's NetFreedom Task Force (previously called the Global Internet Freedom Task Force (GIFT)). The Task Force 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;

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

[2] Testimony of Nicole Wong, Google, before the Senate Committee on the Judiciary Subcommittee on Human Rights and the Law, May 2, 2008.

[3] Secretary of State Hillary Rodham Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World," February 15, 2011, http://www.state.gov/secretary/rm/2011/02/156619.htm.

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

- 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.

Commentators 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 commentators point out that repressive governments could punish or make an example of an individual or company for not following the dictates of that country. This could include harassment, lifting of business licenses, confiscation of assets, or imprisonment. Observers also question what powers the United States may have to respond to such actions, beyond expressing displeasure through official demarches and public statements or through negotiations.[5]

The NetFreedom Task Force

The Task Force is the State Department's policy-coordinating and outreach body for Internet freedom. The members address Internet freedom issues by drawing on the department's multidisciplinary expertise in international communications policy, human rights, democratization, business advocacy, corporate social responsibility, and relevant countries and regions. 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[6]

[5] 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.

[6] 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.

Freedom Online Coalition[7]

The Freedom Online Coalition is a group of governments committed to collaborating to advance Internet freedom. The Coalition provides a forum for governments to coordinate efforts and work with civil society and the private sector to support the ability of individuals to exercise their human rights and freedoms online. Eighteen governments are active in the coalition, including Austria, Canada, Costa Rica, Czech Republic, Finland, France, Estonia, Georgia, Germany, Ghana, Ireland, Kenya, Latvia, the Republic of Maldives, Mexico, Mongolia, The Netherlands, Tunisia, the United Kingdom, the United States, and Sweden.

Digital Defenders Partnership[8]

The Digital Defenders Partnership, a project of the Freedom Online Coalition, is a collaboration among government donors to provide emergency support for Internet users who are under threat for peacefully exercising their rights through new technologies. Together, the United States and other Coalition countries have dedicated more than 2.5 million Euros to this initiative. The U.S. contribution to this initiative builds on the State Department's and USAID's investment of more than $100 million in Internet freedom programming since 2008.

The Partnership has a broad and global scope and awards grants on a flexible basis. Activities from all over the world are eligible for funding as long as they fit the goal of the fund. The Partnership may support activities such as:

- Establishing new internet connections when existing connections have been cut off or are being restricted;
- Personal protection for bloggers and digital activists;
- Development of tools needed to respond adequately to emergencies;
- Development of decentralised, mobile internet applications that can link computers as an independent network (mesh networks);
- Supporting digital activists with secure hosting and DDOS mitigation; and
- Emergency response capacity building.

[7] http://www.humanrights.gov/2012/11/20/freedom-online-joint-action-for-free-expression-on-the-internet/

[8] http://digitaldefenders.org/

The State Department's International Strategy for Cyberspace

In May 2011, the State Department released, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World."[9] This report contains a section called "Internet Freedom: Fundamental Freedoms and Privacy," which sets out a four-pronged strategy to help secure fundamental freedoms and privacy in cyberspace.

Support civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression and association

The State Department supports individual use of digital media to express opinions, share information, monitor elections, expose corruption, and organize social and political movements, and denounce those who harass, unfairly arrest, threaten, or commit violent acts against the people who use these technologies. The department believes that the same protections must apply to ISPs and other providers of connectivity, "who too often fall victim to legal regimes of intermediary liability that pass the role of censoring legitimate speech down to companies."

Collaborate with civil society and nongovernment organizations to establish safeguards protecting their Internet activity from unlawful digital intrusions

The State Department will promote cybersecurity among civil society and nongovernmental organizations to help ensure that freedoms of speech and association are more widely enjoyed in the digital age.

> Cybersecurity is particularly important for activists, advocates, and journalists on the front lines who may express unpopular ideas and opinions, and who are frequently the victims of disruptions and intrusions into their email accounts, websites, mobile phones, and data systems. The United States supports efforts to empower these users to protect themselves, to help ensure their ability to exercise their free expression and association rights on the new technologies of the 21st century.

Encourage international cooperation for effective commercial data privacy protections

The State Department believes that protecting individual privacy is essential to maintaining the trust that sustains economic and social uses of the Internet.

> The United States has a robust record of enforcement of its privacy laws, as well as encouraging multi-stakeholder policy development We are continuing to strengthen the U.S. commercial data privacy framework to keep pace with the rapid changes presented by networked technologies We recognize the role of applying general privacy principles in the commercial context while maintaining the flexibility necessary for innovation. The United States will work toward building mutual recognition of laws that achieve the same objectives and enforcement cooperation to protect privacy and promote innovation.

Ensure the end-to-end interoperability of an Internet accessible to all

The final prong of the strategy is that users should have confidence that the information they send over the Internet will be received as it was intended, anywhere in the world, and that under

[9] U.S. State Department, "International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World," http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

normal circumstances, data will flow across borders without regard for its national origin or destination.

> Ensuring the integrity of information as it flows over the Internet gives users confidence in the network and keeps the Internet open as a reliable platform for innovation that drives growth in the global economy and encourages the exchange of ideas among people around the world. The United States will continue to make clear the benefits of an Internet that is global in nature, while opposing efforts to splinter this network into national intranets that deprive individuals of content from abroad.

Broadcasting Board of Governors

The BBG, through its Internet Anti-Censorship (IAC) Division, directly funds some of the initiatives to develop software and other technologies that allow dissidents to circumvent censorship and surveillance by their governments, and communicate freely. The FY2013 budget for the IAC was $9.1 million. Some of the specific initiatives include[10]—

- development of Android apps, including censorship circumvention tools as well as secure device-to-device sharing of multimedia news and information;
- development of an SMS-based social media network in Cuba;
- ongoing evaluation of circumvention tools; and
- working with the Tor Solutions Group to increase the number of high-speed Tor exit relays and bridges to improve the speed of the Tor network.

In July 2012, in conjunction with Freedom House, the BBG released a report, "Safety on the Line: Exposing the Myth of Mobile Communication Security."[11] The report evaluates the risks and vulnerabilities of mobile phone services and apps in 12 specified countries: the Republic of Azerbaijan, the Republic of Belarus, the People's Republic of China, the Arab Republic of Egypt, the Islamic Republic of Iran, Libya, the Sultanate of Oman, the Kingdom of Saudi Arabia, the Syrian Arab Republic, the Tunisian Republic, the Republic of Uzbekistan, and the Socialist Republic of Vietnam. The study analyzes multiple mobile technologies—including operating systems, applications, and mobile protocol—to determine their capacity to protect security and privacy and to combat censorship and surveillance.

U.S. Industry Activity Promoting Internet Freedom: The Global Network Initiative[12]

In response to criticism, particularly of their operations in China, a group of U.S. information and communications technology companies, along with civil society organizations, investors, and academic entities, formed the Global Network Initiative (GNI) in 2008. The GNI aims to promote

[10] A fact sheet containing information about all the activities by the IAC is available online at http://www.bbg.gov/wp-content/media/2013/05/Anti-Censorship-Fact-Sheet-May-2013.pdf.

[11] http://www.bbg.gov/wp-content/media/2012/07/Safety-on-the-Line.pdf

[12] The GNI 2012 Annual Report is online at http://globalnetworkinitiative.org/sites/default/files/GNI%20Annual%20Report%202012.pdf.

best practices related to the conduct of U.S. companies in countries with poor Internet freedom records.[13] The GNI adopts a self-regulatory approach to promote due diligence and awareness regarding human rights. A set of principles and supporting mechanisms provides guidance to the ICT industry and its stakeholders on how to protect and advance freedom of expression and the right to privacy when faced with pressures from governments to take actions that infringe upon these rights.[14] Companies undergo third-party assessments of their compliance with GNI principles. Although some human rights groups have criticized the GNI's guidelines for being weak or too broad, the GNI's supporters argue that the initiative sets realistic goals and creates real incentives for companies to uphold free expression and privacy.[15]

GNI Report: Protecting Human Rights in the Digital Age

In February 2011, the GNI released the report, "Protecting Human Rights in the Digital Age."[16] In the report, the authors explain the importance of understanding the ICT industry's "freedom of expression and privacy risk drivers" and characteristics that distinguish it from other industry sectors. The report goes on to explain the characteristics that exist across five spheres and have implications for how to best protect and advance human rights in the industry:

- End user—plays a significant role in the human rights impact of ICT
- Legal frameworks—can move more slowly than ICT product and service development
- Jurisdictional complexity—increasingly significant as information becomes global and data flows across borders
- Technological complexity—new products and services are continually introduced, often with unpredictable consequences for human rights
- B2B relationships with enterprise and government customers—with whom ICT companies often co-design products and services.

The GNI provides direction and guidance to companies on how to respond to government demands to remove, filter, or block content, and how to respond to law enforcement agency demands to disclose personal information. These types of risk drivers will be relevant for companies that hold significant amounts of personal information and/or act as gatekeepers to content, primarily telecommunications services providers and internet services companies.

The report sets out the following "risk drivers" across eight segments of the ICT industry:

- Telecommunications Services—risk drivers include requirements to assist law enforcement agencies in investigations

[13] The GNI website is online at http://www.globalnetworkinitiative.org/index.php. The 2011 GNI annual report is available online at http://www.globalnetworkinitiative.org/files/GNI_2011_Annual_Report.pdf.

[14] http://www.globalnetworkinitiative.org/index.php

[15] Elisa Massimino, Human Rights First, "Judge the Global Network Initiative by How It Judges Companies," March 31, 2011; Douglass MacMillan, "Google, Yahoo Criticized over Foreign Censorship," *BusinessWeek*, March 13, 2009.

[16] Global Network Initiative, "Protecting Human Rights in the Digital Age," February 2011, http://www.globalnetworkinitiative.org/cms/uploads/1/BSR_ICT_Human_Rights_Report.pdf

- Cell Phones and Mobile Devices—location-based services such as mapping or advertising can present new sources of security and privacy risks
- Internet Services—companies can receive demands to remove, block, or filter content, or deactivate individual user accounts
- Enterprise Software, Data Storage, and IT Services—companies hosting data "in the cloud" may increasingly be gatekeepers to law enforcement requests or provide service to high-risk customers
- Semiconductors and Chips—hardware can be configured to allow remote access, which may present security and privacy risks
- Network Equipment—where functionality necessarily allows content to be restricted or data to be collected by network managers
- Consumer Electronics—pressure may exist to pre-install certain types of software to restrict access to content or allow for surveillance
- Security Software—risk drivers may include increasing pressure to offer simpler means of unscrambling encrypted information.

The GNI report concludes by highlighting four key topics that any ongoing dialogue about the technology industry should likely address: relationships with governments; designing future networks; implementing due diligence; and engaging employees, users, and consultants.

Legislative Activity in the 113th Congress

In the 113th Congress, one piece of legislation has been introduced and one hearing held.

Legislation

Representative Christopher Smith introduced the *Global Online Freedom Act of 2013*, H.R. 491, on February 4, 2013. The bill was referred to House Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations on February 25, 2013. Among other goals, H.R. 491 would:

- Make it U.S. policy to deter U.S. businesses from cooperating with Internet-restricting countries in effecting online censorship.
- Amend the Foreign Assistance Act of 1961 to require assessments of electronic information freedom in each foreign country.
- Direct the Secretary of State to annually designate Internet-restricting countries.
- Amend the Securities Exchange Act of 1934 to require each Internet communications services company that operates in an Internet-restricting country to include in its annual report information relating to human rights due diligence, policies pertaining to the collection of personally identifiable information, and restrictions on Internet search engines or content hosting services.
- Amend the Export Administration Act of 1979 to direct the Secretary of Commerce to establish a list of technologies (and related goods) that would assist

censorship or surveillance efforts by a foreign government and prohibit export of those items to a government in any Internet-restricting country.

Hearings

"Fighting for Internet Freedom: Dubai and Beyond" was held on February 5, 2013, by the House Committee on Energy and Commerce's Subcommittee on Communications and Technology.[17]

Legislative Activity in the 112th Congress

In the 112th Congress, there was one piece of legislation introduced and two hearings held.

Legislation

Representative Christopher Smith introduced the *Global Online Freedom Act of 2011*, H.R. 3605, on December 12, 2011. The bill was ordered to be reported, as amended, on March 27, 2012. H.R. 3605 was substantially the same as H.R. 491 that has been introduced in the 113th Congress.

Hearings

Two hearings were also been held on the subject of Global Internet Freedom.

- Congressional-Executive Commission on China, *China's Censorship of the Internet and Social Media: The Human Toll and Trade Impact*, November 17, 2011.
- House Committee on Foreign Affairs, Subcommittee on Africa, Global Health, and Human Rights, *Promoting Global Internet Freedom*, December 8, 2011.

[17] http://energycommerce.house.gov/hearing/fighting-for-internet-freedom-dubai-and-beyond

Appendix A. For Further Reading

"Leaping over the Firewall: A Review of Censorship Circumvention Tools"
Freedom House
April 2011
http://www.freedomhouse.org/template.cfm?page=383&report=97
Report

"Freedom on the Net 2011: A Global Assessment of Internet and Digital Media"
Freedom House
September 2012
http://www.freedomhouse.org/uploads/fotn/2011/FOTN2011.pdf
Report
(Main report page: http://www.freedomhouse.org/report/freedom-net/freedom-net-2012)

"Protecting Human Rights in the Digital Age"
Global Network Initiative
February 2011
http://www.globalnetworkinitiative.org/cms/uploads/1/BSR_ICT_Human_Rights_Report.pdf
Report

"The Political Power of Social Media: Technology, the Public Sphere, and Political Change"
Foreign Affairs (Journal of the Council on Foreign Relations), by Clay Shirky
January/February 2011
http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media
*Full article not available online.
Article

Appendix B. Methods/Technologies Used to Monitor and Censor Websites and Web-Based Communications[18]

There are four different types of targets that are censored:

- Services, e.g., email, the web, peer-to-peer, social networking service
- Content, e.g., hate speech, child pornography, gambling, human-rights organizations, independent news sites, political opposition sites
- Activities, e.g., illegal music downloads, spam, political organizing by opposition groups in repressive regimes.

These targets can be censored using the methods listed below.

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.

[18] Adapted from "Leaping Over the Firewall: A Review of Censorship Circumvention Tools," Freedom House, April 2011, http://www.freedomhouse.org/template.cfm?page=383&report=97 ;"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.

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 FTP transfers are most often sent through a specific communications port, a government 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 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 C. Technologies Used to Circumvent Censorship[19]

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

[19] 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
Specialist in Internet and Telecommunications Policy
pfigliola@crs.loc.gov, 7-2508

Acknowledgments

Casy Addis, Thomas Lum, Kennon H. Nakamura, and Gina Stevens contributed to a previous version of this report.