

Promoting Global Internet Freedom: Policy and Technology

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy

January 17, 2012

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.

Current legislation under consideration by the 112th 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 about federal and private sector efforts to promote and support global Internet freedom, a description of Internet freedom legislation from the 112th Congress, and suggestions for further reading on this topic. Two appendixes describe censorship and circumvention technologies.

Contents

Introduction 1
Doing Business with Repressive Regimes: U.S. Industry Dilemma 1
U.S. State Department: Promoting Internet Freedom 2
The NetFreedom Task Force 3
The State Department's International Strategy for Cyberspace 4
U.S. Industry Activity Promoting Internet Freedom: The Global Network Initiative 5
GNI Report: Protecting Human Rights in the Digital Age 7
Legislative Activity in the 112th Congress 8
For Further Reading 9

Appendixes

Appendix A. Methods/Technologies Used to Monitor and Censor Websites and Web-Based Communications 11
Appendix B. 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 (see **Appendix A** for a description of methods). 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 (see **Appendix B**).

The restriction of Internet freedom by foreign governments creates a tension between U.S. policymakers 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 112th Congress, 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. 1389), 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. 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. State Department: Promoting Internet Freedom

The State Department works to advance Internet freedom as an aspect of the universal rights of freedom of expression and the free flow of information. On February 15, 2011, Secretary Clinton reconfirmed the U.S. commitment to "protect and defend a free and open Internet."[3] Secretary Clinton has outlined 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;
- 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;

[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.

- 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]

- 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;

[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.

- 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.

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."[7] 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

[7] 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.

> 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 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.

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

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.[8] The 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 and supporting mechanisms provide guidance to the information and communications technology (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.

Governments are not members of the GNI, but are encouraged to support the principles and encourage their adoption. U.S. companies 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 but that were involved in its development include Amnesty International and Reporters Without Borders. Reporters Without Borders remains skeptical about how much change GNI can effect.[9] It has 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.

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

[9] Reporters Without Borders, ''Why Reporters Without Borders Is Not Endorsing the Global Principles on Freedom of Expression and Privacy for ICT Companies Operating in Internet Restricting Countries,'' October 28, 2008, http://www.rsf.org/article.php3?id_article=29117.

The GNI acknowledges that the rights of privacy and 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

- require governments to follow local legal processes;
- interpret the governmental authority's jurisdiction to minimize the negative effect; and
- interpret government demands so as to minimize the negative effect, when required to restrict communications or remove content.

Companies also commit to encourage governments to

- be specific, transparent, and consistent in the demands issued to restrict freedom of expression online; and
- limit demands to those consistent with international laws and standards.

Companies that participate also 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 are to be phased in over three stages:

- In Phase One (ended December 2010) each participating company established 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 conducted 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 is supposed to submit an annual report to the Organization. The assessors are then supposed to prepare reports explaining each company's responses to government demands, evaluating the effectiveness of the company's responses. Each company is given the opportunity to respond to the assessor's draft and final report. The Board of the Organization plans to assess whether the company is in compliance with the Principles and make its determination public. The Board of the Organization plans to publish an annual report assessing each participating company's compliance with the Principles.

GNI Report: Protecting Human Rights in the Digital Age

In February 2011, the GNI released the report, "Protecting Human Rights in the Digital Age."[10] 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
- 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

[10] 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

- 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 112th Congress

Two bills and one resolution have been introduced in the 112th Congress related to global Internet freedom.

H.R. 1389, *Global Online Freedom Act of 2011*. Introduced by Representative Christopher Smith. Referred to the House Committee on Foreign Affairs and the House Committee on Energy and Commerce on April 6, 2011; referred to the House Committee on Foreign Affairs Subcommittee on Africa, Global Health, and Human Rights on May 13, 2001. This bill is identical to H.R. 2271 that was introduced in the 111th Congress. H.R. 1389 would:

- Make 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.
- Express 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.
- Amend the Foreign Assistance Act of 1961 to require assessments of electronic information freedom in each foreign country.
- Establish in the Department of State the Office of Global Internet Freedom (OGIF).
- Direct 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.
- Require 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.
- Require U.S. businesses to report to the OGIF certain Internet censorship information involving Internet-restricting countries.

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

S. 879 and H.R. 1714, *Iran Human Rights and Democracy Promotion Act of 2011*. These bills were both introduced on May 4, 2011, by Senator Mark Steven Kirk in the Senate and by Representative Robert Dold in the House. The bills were referred to the Senate Committee on Foreign Relations and the House Committee on Foreign Affairs.[11] Among other purposes, these bills would require the President to submit to Congress a comprehensive strategy to promote Internet freedom and access to information in Iran.

H.Res. 29, *Calling for Internet freedom in Vietnam*. Introduced by Representative Loretta Sanchez on January 7, 2011, and referred to the House Committee on Foreign Affairs Subcommittee on Africa, Global Health, and Human Rights on March 1, 2011.

This resolution would:

- Support 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.
- Call 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; and (2) become a responsible member state of the international community by respecting individuals' freedom of speech, freedom of press, and freedom of political association.

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
April 2011
http://www.freedomhouse.org/uploads/fotn/2011/FOTN2011.pdf
Report

[11] H.R. 1714 was also referred to the House Committees on Financial Services, the Judiciary, and Ways and Means.

"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

Related:

"Social Media and Revolution"
The Brian Lehrer Show
January 2011
http://www.wnyc.org/shows/bl/2011/jan/19/wikileaks-revolution/
Audio Transcript

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

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

Appendix A. Methods/Technologies Used to Monitor and Censor Websites and Web-Based Communications[12]

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.

[12] 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 B. Technologies Used to Circumvent Censorship[13]

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

[13] 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.