110TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 110–481
Part 1

GLOBAL ONLINE FREEDOM ACT OF 2007

DECEMBER 10, 2007.—Ordered to be printed

Mr. LANTOS, from the Committee on Foreign Affairs, submitted the following

R E P O R T

[To accompany H.R. 275]

[Including cost estimate of the Congressional Budget Office]

The Committee on Foreign Affairs, to whom was referred the bill (H.R. 275) to promote freedom of expression on the Internet, to protect United States businesses from coercion to participate in repression by authoritarian foreign governments, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

TABLE OF CONTENTS

THE AMENDMENT

The amendment is as follows:
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Global Online Freedom Act of 2007".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) Freedom of speech and freedom of the press are fundamental human rights, and free flow of information on the Internet is protected in Article 19 of the Universal Declaration of Human Rights, which guarantees freedom to "receive and impart information and ideas through any media regardless of frontiers".

(2) The Internet has been a success because it quickly provides information to its more than one billion users globally.

(3) The growth of the Internet and other information technologies can be a force for democratic change if the information is not subject to political censorship.

(4) The Internet has played a role in bringing international attention to issues the discussion of which are forbidden by authoritarian foreign governments, such as attempts by the Government of the People's Republic of China to suppress news of the severe acute respiratory syndrome (SARS) outbreak in 2004.

(5) Authoritarian foreign governments such as the Governments of Belarus, Cuba, Ethiopia, Iran, Laos, North Korea, the People's Republic of China, Tunisia, and Vietnam, among others, block, restrict, and monitor the information their citizens try to obtain.

(6) Web sites that provide uncensored news and information, such as the Web sites of the Voice of America and Radio Free Asia, are routinely blocked in such countries.

(7) In June 2003, the Government of the Socialist Republic of Vietnam arrested, convicted of "spying", and sentenced to 13 years imprisonment and 3 years house arrest (later reduced on appeal to 5 years imprisonment and 3 years house arrest) Dr. Pham Hong Son after he translated an Internet article titled "What is Democracy" from the Web site of the United States Embassy in Vietnam.

(8) According to the Department of State's Country Reports on Human Rights Practices, the Government of Vietnam in 2004 tightened control of the Internet, requiring Internet agents, such as "cyber cafes", to register the personal information of their customers and store records of Internet sites visited by customers. The Vietnamese Government also monitored electronic mail, searched for sensitive key words, and regulated Internet content.

(9) The Government of the People's Republic of China has employed censorship of the Internet in violation of Article 35 of the Chinese Constitution, which guarantees freedom of speech and freedom of the press.

(10) This censorship by the Chinese Government allows that Government to promote a xenophobic—and at times particularly anti-American—Chinese nationalism, the long-term effect of which will be deleterious to United States efforts to improve the relationship between the United States and China.

(11) Technology companies in the United States that operate in countries controlled by authoritarian foreign governments have a moral responsibility to comply with the principles of the Universal Declaration of Human Rights.

(12) Technology companies in the United States have succumbed to pressure by authoritarian foreign governments to provide such governments with information about Internet users that has led to the arrest and imprisonment of "cyber dissidents", in violation of the corporate responsibility of such companies to protect and uphold human rights.

(13) Technology companies in the United States have provided technology and training to authoritarian foreign governments which have been used by such governments in filtering and blocking information that promotes democracy and freedom.

(14) Technology companies in the United States should develop standards by which they can conduct business with authoritarian foreign governments while protecting human rights to freedom of speech and freedom of expression.

SEC. 3. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—Except as otherwise provided in this Act, the term "appropriate congressional committees" means—

(A) the Committee on Foreign Affairs of the House of Representatives; and

(B) the Committee on Foreign Relations of the Senate.

(2) FOREIGN OFFICIAL.—

(A) IN GENERAL.—The term "foreign official" means—

(i) any officer or employee of a foreign government or any department, agency, state-owned enterprise, or instrumentality thereof; or

(ii) any person acting in an official capacity for or on behalf of any such government or department, agency, state-owned enterprise, or instrumentality.

(B) STATE-OWNED ENTERPRISE.—For purposes of subparagraph (A), the term "state-owned enterprise" means a commercial entity in which a foreign government owns, directly or indirectly, more than 50 percent of the outstanding capital stock or other beneficial interest in such commercial entity.

(3) INTERNET.—The term "Internet" means the combination of computer facilities, telecommunications facilities, electromagnetic transmission media, and related equipment and software, comprising the interconnected worldwide network of computer networks that employ the Transmission Control Protocol/Internet Protocol or any successor protocol to transmit information.

(4) INTERNET CONTENT HOSTING SERVICE.—The terms "Internet content hosting service" and "content hosting service" mean a service that—

(A) stores, through electromagnetic or other means, electronic data, including the content of Web pages, electronic mail, documents, images, audio and video files, online discussion boards, and Web logs; and

(B) makes such data available via the Internet.

(5) INTERNET JAMMING.—The term "Internet jamming" means jamming, censoring, blocking, monitoring, or restricting access to the Internet, or to content made available via the Internet, by using technologies such as firewalls, filters, and "black boxes".

(6) INTERNET-RESTRICTING COUNTRY.—The term "Internet-restricting country" means a country designated by the President pursuant to section 105(a) of this Act.

(7) INTERNET SEARCH ENGINE.—The term "Internet search engine" or "search engine" means a service made available via the Internet that, on the basis of query consisting of terms, concepts, questions, or other data input by a user, searches information available on the Internet and returns to the user a means, such as a hyperlinked list of Uniform Resource Identifiers, of locating, viewing, or downloading information or data available on the Internet relating to that query.

(8) LEGITIMATE FOREIGN LAW ENFORCEMENT PURPOSES.—

(A) IN GENERAL.—The term "legitimate foreign law enforcement purposes" means for purposes of enforcement, investigation, or prosecution by a foreign official based on a publicly promulgated law of reasonable specificity that proximately relates to the protection or promotion of the health, safety, or morals of the citizens of that jurisdiction.

(B) RULE OF CONSTRUCTION.—For purposes of this Act, the control, suppression, or punishment of peaceful expression of political or religious opinion, which is protected by Article 19 of the International Covenant on Civil and Political Rights, does not constitute a legitimate foreign law enforcement purpose.

(9) PERSONALLY IDENTIFIABLE INFORMATION.—The term "personally identifiable information"—

(A) includes any information described in section 2703(c)(2) of title 18, United States Code; and

(B) does not include—

(i) any traffic data (as such term is defined in section 201(b) of this Act); or

(ii) any record of aggregate data that does not identify particular persons.

(10) SUBSTANTIAL RESTRICTIONS ON INTERNET FREEDOM.—The term "substantial restrictions on Internet freedom" means actions that restrict or punish the free availability of information via the Internet for reasons other than legitimate foreign law enforcement purposes, including—

(A) deliberately blocking, filtering, or censoring information available via the Internet based on its peaceful political or religious content; or

(B) persecuting, prosecuting, or otherwise punishing an individual or group for posting or transmitting peaceful political or religious opinions via the Internet, including by electronic mail.

(11) UNITED STATES BUSINESS.—The term "United States business" means—

(A) any corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship that—

(i) has its principal place of business in the United States; or

(ii) is organized under the laws of a State of the United States or a territory, possession, or commonwealth of the United States;

(B) any issuer of a security registered pursuant to section 12 of the Securities Exchange Act of 1934 (15 U.S.C. 78l); and

(C) any foreign subsidiary of an entity described in subparagraph (A) or (B) to the extent such entity—

(i) controls the voting shares or other equities of the foreign subsidiary; or

(ii) authorizes, directs, controls, or participates in acts carried out by the foreign subsidiary that are prohibited by this Act.

(12) UNITED STATES-SUPPORTED CONTENT.—The term "United States-supported content" means content that is created or developed, in whole or in part, by a United States-supported information entity.

(13) UNITED STATES-SUPPORTED INFORMATION ENTITY.—The term "United States-supported information entity" means—

(A) any authority of the Government of the United States; and

(B) any entity that—

(i) receives grants from the Broadcasting Board of Governors to carry out international broadcasting activities in accordance with the United States International Broadcasting Act of 1994 (title III of Public Law 103–236; 22 U.S.C. 6201 et seq.);

(ii) exists within the Broadcasting Board of Governors and carries out nonmilitary international broadcasting activities supported by the Government of the United States in accordance with such Act; or

(iii) receives grants or other similar funding from the Government of the United States to carry out any information dissemination activities.

(14) UNITED STATES-SUPPORTED WEB SITE.—The term "United States-supported Web site" means a location on the World Wide Web that is owned or managed by, or is registered to, a United States-supported information entity.

SEC. 4. SEVERABILITY.

If any provision of this Act, or the application of such provision to any person or circumstance, is held invalid, the remainder of this Act, and the application of such provision to other persons not similarly situated or to other circumstances, shall not be affected by such invalidation.

TITLE I—PROMOTION OF GLOBAL INTERNET FREEDOM

SEC. 101. STATEMENT OF POLICY.

It shall be the policy of the United States—

(1) to promote as a fundamental component of United States foreign policy the right of every individual to freedom of opinion and expression, including the right to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers;

(2) to use all appropriate instruments of United States influence, including diplomacy, trade policy, and export controls, to support, promote, and strengthen principles, practices, and values that promote the free flow of information, including through the Internet and other electronic media; and

(3) to deter any United States business from cooperating with officials of Internet-restricting countries in effecting the political censorship of online content.

SEC. 102. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) the President should through bilateral, and where appropriate, multilateral activities, seek to obtain the agreement of other countries to promote the goals and objectives of this Act and to protect Internet freedom; and

(2) to the extent that a United States business empowers or assists an authoritarian foreign government in its efforts to restrict online access to the Web sites of Radio Free Asia, the Voice of America, or other United States-supported Web sites and online access to United States Government reports such as the Annual Country Reports on Human Rights Practices, the Annual Reports on International Religious Freedom, and the Annual Trafficking in Human Persons Reports, or to identify individual Internet users, that business is working contrary to the foreign policy interests of the United States, and is undercutting United States taxpayer-funded efforts to promote freedom of information for all people, including those in undemocratic and repressive societies.

SEC. 103. ANNUAL COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES.

(a) REPORT RELATING TO ECONOMIC ASSISTANCE.—Section 116 of the Foreign Assistance Act of 1961 (22 U.S.C. 2151n) is amended by adding at the end the following new subsection:

"(g)(1) The report required by subsection (d) shall include an assessment of the freedom of electronic information in each foreign country. Such assessment shall include the following:

"(A) An assessment of the general extent to which Internet access is available to and used by citizens in that country.

"(B) An assessment of the extent to which government authorities in that country attempt to filter, censor, or otherwise block Internet content, as well as a description of the means by which they attempt to block such content.

"(C) A description of known instances in which government authorities in that country have persecuted, prosecuted, or otherwise punished a person or group for the peaceful expression of political, religious, or dissenting views via the Internet, including electronic mail.

"(D) A description of known instances in which government authorities in that country have sought to collect, request, obtain or disclose the personally identifiable information of a person in connection with that person's communication of ideas, facts or views where such communication would be protected by the International Covenant on Civil and Political Rights.

"(2) In compiling data and making assessments for the purposes of paragraph (1), United States diplomatic mission personnel shall consult with human rights organizations, technology and internet companies and other appropriate nongovernmental organizations.".

(b) REPORT RELATING TO SECURITY ASSISTANCE.—Section 502B of the Foreign Assistance Act of 1961 (22 U.S.C. 2304) is amended by adding at the end the following new subsection:

"(i)(1) The report required by subsection (b) shall include an assessment of the freedom of electronic information in each foreign country. Such assessment shall include the following:

"(A) An assessment of the general extent to which Internet access is available to and used by citizens in that country.

"(B) An assessment of the extent to which government authorities in that country attempt to filter, censor, or otherwise block Internet content, as well as a description of the means by which they attempt to block such content.

"(C) A description of known instances in which government authorities in that country have persecuted, prosecuted, or otherwise punished a person or group for the peaceful expression of political, religious, or dissenting views via the Internet, including electronic mail.

"(D) A description of known instances in which government authorities in that country have sought to collect, request, obtain or disclose the personally identifiable information of a person in connection with that person's

communication of ideas, facts or views where such communication would be protected by the International Covenant on Civil and Political Rights.

"(2) In compiling data and making assessments for the purposes of paragraph (1), United States diplomatic mission personnel shall consult with human rights organizations, technology and internet companies, and other appropriate nongovernmental organizations.".

SEC. 104. OFFICE OF GLOBAL INTERNET FREEDOM.

(a) ESTABLISHMENT.—There is established in the Department of State the Office of Global Internet Freedom (in this section referred to as the "Office").

(b) DUTIES.—In addition to such other responsibilities as the President may assign, the Office shall—

(1) serve as the focal point for interagency efforts to protect and promote freedom of electronic information abroad;

(2) develop and ensure the implementation of a global strategy and programs to combat state-sponsored and state-directed Internet jamming by authoritarian foreign governments, and the intimidation and persecution by such governments of their citizens who use the Internet;

(3) provide assistance to the President in connection with the annual designation of Internet-restricting countries required by section 105(a) of this Act;

(4) beginning not later than 180 days after the date of the enactment of this Act—

(A) identify key words, terms, and phrases relating to human rights, democracy, religious free exercise, and peaceful political dissent, both in general and as specifically related to the particular context and circumstances of each Internet-restricting country; and

(B) maintain, update, and make publicly available on a regular basis the key words, terms, and phrases identified pursuant to subparagraph (A);

(5) establish mechanisms to collect the information required to be reported by sections 116(g) and 502B(i) of the Foreign Assistance Act of 1961 (as added by section 103 of this Act) and sections 203 and 204 of this Act;

(6) establish a regularized consultative process with appropriate technology companies involved in providing, maintaining, or servicing the Internet, human rights organizations, academic experts, and others to develop a voluntary code of minimum corporate standards related to Internet freedom, and to consult with such companies, organizations, experts, and others regarding new technologies and the implementation of appropriate policies relating to such technologies; and

(7) advise the appropriate congressional committees of legislative action that may be necessary to keep the provisions of this Act and the amendments made by this Act relevant to changing technologies.

(c) COOPERATION OF OTHER FEDERAL DEPARTMENTS AND AGENCIES.—Each department and agency of the Government of the United States, including the Department of Commerce, the Office of the United States Trade Representative, the Department of Justice, the International Broadcasting Bureau, and the Office of the Director of National Intelligence, shall—

(1) cooperate fully with, and assist in the implementation of, the duties of the Office described in subsection (b), including the strategy developed by the Office pursuant to paragraph (2) of subsection (b); and

(2) make such resources and information available to the Office on a nonreimbursable basis as is necessary to achieve the purposes of this Act and the amendments made by this Act.

(d) DEFINITION.—In this section, the term "appropriate congressional committees" means—

(1) the Committee on Foreign Affairs and the Committee on Energy and Commerce of the House of Representatives; and

(2) the Committee on Foreign Relations and the Committee on Commerce, Science, and Transportation of the Senate.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Office to carry out this section $50,000,000 for each of the fiscal years 2008 and 2009.

SEC. 105. ANNUAL DESIGNATION OF INTERNET-RESTRICTING COUNTRIES; REPORT.

(a) DESIGNATION.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, the President shall designate Internet-restricting countries for purposes of this Act.

(2) STANDARD.—A foreign country shall be designated as an Internet-restricting country if the President determines that the government of the country is

directly or indirectly responsible for a systematic pattern of substantial restrictions on Internet freedom during the preceding 1-year period.

(b) REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, the President shall transmit to the appropriate congressional committees a report that contains the following:

(A) The name of each foreign country that at the time of the transmission of the report is designated as an Internet-restricting country pursuant to subsection (a).

(B) An identification of each government agency and quasi-government organization responsible for the substantial restrictions on Internet freedom in each foreign country designated as an Internet-restricting country pursuant to subsection (a).

(C) A description of efforts by the United States to counter the substantial restrictions on Internet freedom referred to in subparagraph (B).

(2) FORM.—The information required by paragraph (1)(C) of the report may be provided in a classified form if necessary.

(3) INTERNET AVAILABILITY.—All unclassified portions of the report shall be made publicly available on the Internet Web site of the Department of State.

TITLE II—MINIMUM CORPORATE STANDARDS FOR ONLINE FREEDOM

SEC. 201. PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION.

(a) PROHIBITION OF LOCATING PERSONALLY IDENTIFIABLE INFORMATION IN INTERNET-RESTRICTING COUNTRIES.—A United States business may not locate, within a designated Internet-restricting country, any electronic communication that contains any personally identifiable information.

(b) DEFINITIONS.—In this section:

(1) TITLE 18 DEFINITIONS.—The terms "electronic communication", "electronic communications system", "electronic storage", and "contents" have the meanings given such terms in section 2510 of title 18, United States Code.

(2) LOCATE.—The term "locate" includes, with respect to an electronic communication—

(A) computer storage or processing by facilities of a remote computing service, as such term is defined in section 2711 of title 18, United States Code;

(B) electronic storage by any electronic or computer server or facility of an electronic communications system; and

(C) any other storage by any electronic or computer server or facility.

(3) TRAFFIC DATA.—The term "traffic data" means, with respect to an electronic communication, any information contained in or relating to such communication that is processed for the purpose of the conveyance of the communication by an electronic communications system or for the billing thereof, including any Internet Protocol address or other means of identifying a location within an electronic communications system, but that does not by itself identify a particular person. Such term does not include the contents of any electronic communication.

SEC. 202. INTEGRITY OF PERSONALLY IDENTIFIABLE INFORMATION.

(a) USER PROTECTION.—If a United States business collects or obtains personally identifiable information through the provision of products or services on the Internet, such business may not provide such information to any foreign official of an Internet-restricting country, except for legitimate foreign law enforcement purposes as determined by the Department of Justice.

(b) USE OF ESTABLISHED LEGAL CHANNELS.—Any information that may be provided under subsection (a) for legitimate foreign law enforcement purposes may only be provided through established legal channels as determined by the Department of Justice.

(c) PRIVATE RIGHT OF ACTION.—Any person aggrieved by a violation of this section may bring an action for damages, including punitive damages, or other appropriate relief in the appropriate district court of the United States, without regard to the amount in controversy, and without regard to the citizenship of the parties.

SEC. 203. TRANSPARENCY REGARDING SEARCH ENGINE FILTERING.

Any United States business that creates, provides, or hosts an Internet search engine shall provide the Office of Global Internet Freedom, in a format and with a frequency to be specified by the Office, with all terms and parameters used to filter,

limit, or otherwise affect the results provided by the search engine that are implemented—

(1) at the request of, or by reason of any other direct or indirect communication by, any foreign official of an Internet-restricting country; or

(2) to comply with a policy or practice of restrictions on Internet freedom in an Internet-restricting country.

SEC. 204. TRANSPARENCY REGARDING INTERNET CENSORSHIP.

(a) PROVISION OF URLS.—Any United States business that maintains an Internet content hosting service shall provide the Office of Global Internet Freedom, in a format and with a frequency to be specified by the Office, with the Uniform Resource Locators (URLs) of all data and content that such business has, under the circumstances set forth in subsection (b)—

(1) removed from the content hosting service of such business;

(2) blocked from availability on the Internet; or

(3) blocked from transmission via the Internet into or within an Internet-restricting country.

(b) CIRCUMSTANCES.—The circumstances referred to in subsection (a) are that the United States business took the action under subsection (a)—

(1) at the request of, or by reason of any other direct or indirect communication by, any foreign official of an Internet-restricting country; or

(2) in order to comply with a policy or practice of restrictions on Internet freedom in an Internet-restricting country.

SEC. 205. PROTECTION OF UNITED STATES-SUPPORTED ONLINE CONTENT.

A United States business that maintains an Internet content hosting service may not conduct Internet jamming of a United States-supported Web site or United States-supported content in an Internet-restricting country.

SEC. 206. PENALTIES.

(a) CIVIL PENALTIES.—(1)(A) Any United States business that violates section 202(a) shall be subject to a civil penalty of not more than $2,000,000 imposed in an action brought by the Attorney General.

(B) Any officer, director, employee, or agent, or stockholder of a United States business, who is acting on behalf of that business concern and who violates section 202(a), shall be subject to a civil penalty of not more $100,000 imposed in an action brought by the Attorney General.

(2) Any United States business that violates section 201, 203, 204, or 205, or any officer, director, employee, or agent, or stockholder of a United States business, who is acting on behalf of that business concern and who violates section 201, 203, 204, or 205, shall be subject to a civil penalty of not more than $10,000 imposed in an action brought by the Attorney General.

(b) CRIMINAL PENALTIES.—(1)(A) Any United States business that willfully violates, or willfully attempts to violate, section 202(a) shall be fined not more than $2,000,000.

(B) Any officer, director, employee, or agent, or stockholder of a United States business, who is acting on behalf of that business concern, and who willfully violates, or willfully attempts to violate, section 202(a), shall be fined not more than $100,000, or imprisoned not more than 5 years, or both.

(2)(A) Any United States business that willfully violates, or willfully attempts to violate, section 201, 203, 204, or 205 shall be fined not more than $10,000.

(B) Any officer, director, employee, or agent, or stockholder of a United States business, who is acting on behalf of that business concern and who willfully violates, or willfully attempts to violate, section 201, 203, 204, or 205, shall be fined not more than $10,000, or imprisoned not more than 1 year, or both.

(c) PAYMENT OF FINES.—Whenever a fine is imposed under subsection (a) or (b) upon any officer, director, employee, agent, or stockholder of a United States business, the fine may not be paid, directly or indirectly, by the United States business.

SEC. 207. PRESIDENTIAL WAIVER.

(a) IN GENERAL.—Subject to subsection (b), the President may waive the application of any of the provisions of sections 201 through 205 with respect to a United States business or an Internet-restricting country, if the President determines and so reports to the appropriate congressional committees that—

(1) the government of the country has ceased the activities giving rise to the designation of the country as an Internet-restricting country;

(2) the exercise of such waiver authority would further the purposes of this Act; or

(3) the important national interest of the United States requires the exercise of such waiver authority.

(b) CONGRESSIONAL NOTIFICATION.—Not later than the date of the exercise of a waiver under subsection (a), the President shall notify the appropriate congressional committees of the waiver or the intention to exercise the waiver, together with a detailed justification for the waiver.

TITLE III—EXPORT CONTROLS FOR INTERNET-RESTRICTING COUNTRIES

SEC. 301. FEASIBILITY STUDY ON ESTABLISHMENT OF EXPORT CONTROLS.

Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce, in consultation with the Secretary of State, shall complete a feasibility study regarding the development of export controls and export license requirements regarding the export of any item subject to sections 730 through 774 of title 15, Code of Federal Regulations (commonly known as the "Export Administration Regulations") to an end user in an Internet-restricting country for the purpose, in whole or in part, of facilitating substantial restrictions on Internet freedom.

SEC. 302. REPORT.

Not later than 30 days after the end of the 180-day period described in section 301, the Secretary of Commerce, in consultation with the Secretary of State, shall submit to the appropriate congressional committees a report describing the actions taken to carry out section 301.

SUMMARY

H.R. 275, the Global Online Freedom Act of 2007 (the "Act") establishes procedures to maximize Internet freedom in countries that the President designates as Internet-restricting countries. The Act establishes procedures that American companies, the State Department and Internet-restricting countries must follow to prevent the disclosure of political dissidents' personal information, to prevent Internet censorship and to prohibit jamming of U.S. Government-generated Internet content. The Act creates a State Department office to collect information about and report on global internet freedom. It requires transparency in filtering of search terms in Internet search engines. It also requires a study concerning export controls related to technology that supports Internet censorship.

BACKGROUND AND PURPOSE FOR THE LEGISLATION

H.R. 275 responds to the increasing use of the Internet by authoritarian governments around the world as a tool of repression. The World Wide Web was designed to be a tool to promote the free flow of information, but, in the hands of certain governments and companies, the Internet has been used as a tool of censorship.

One of the most serious problems that the Act seeks to redress is the role of American companies with respect to the jailing of political dissidents. In many nations, American companies have cooperated with security forces in the investigation, arrest and punishment of political dissidents. American companies have disclosed to security forces in repressive regimes the content of private communications and the identity of their Internet customers, sometimes leading to the arrest and conviction of political dissidents. In some cases, this cooperation has been done willingly and for profit. In others, it has occurred in response to subpoenas or due to the fear of sanctions imposed by local law. The victims in these cases have been jailed for expressing political views on the Internet, specifically for exercising their rights to free expression protected by

the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights.

China's jailing of journalist Shi Tao is an example of the problems that H.R. 275 seeks to correct. Shi Tao is serving a 10-year sentence for disclosure of state secrets after he forwarded to a U.S.-based pro-democracy website a Chinese government directive ordering journalists not to report on the 15th anniversary of the 1989 Tiananmen Square massacre. Police tracked down Shi Tao through his Yahoo! e-mail account that was used to forward the censorship order. Responding to a request from the Beijing State Security Bureau, Yahoo! turned over to the Chinese security services Shi's Yahoo! e-mail account details, including the IP address and location where he logged on to the Yahoo! service. Using those details, the Chinese security services identified the e-mails as coming from Shi's office at the newspaper "Contemporary Business News." The verdict convicting Shi cited the information Yahoo! provided as central to his arrest and conviction. Information provided to the Chinese security authorities by Yahoo! was also cited in verdicts convicting other Chinese dissidents of crimes involving state secrets and subversion, including Wang Xiaoning, Li Zhi and Jiang Lianjun. Many others have been arrested based on information obtained through investigations of on-line activities, even if the verdicts jailing them did not single out information provided by a particular American company. Among them was Dr. Pham Hong Son, sentenced to 13 years imprisonment in June 2003 after he translated an Internet article entitled "What is Democracy?" from the Website of the U.S. Embassy in Vietnam. Similar convictions have taken place in other countries with repressive governments and in countries that do not recognize internationally respected rights of free expression.

The Act also addresses the problem of American companies helping certain authoritarian governments to censor the Internet and to use the Internet as a tool to jail political dissidents. Cisco Systems, Fortinet, Websense Inc., Secure Computing Corp. and Blue Coat Systems Inc. are among companies that academics have identified as providing technology to support Internet censorship in countries such as Iran, Burma, China, Tunisia, Saudi Arabia and the United Arab Emirates. This technology may be used to identify dissidents. Or it may be used to filter out key terms from email and Internet traffic. These technologies can also be used to facilitate search engine censorship. In China, for example, a search for the terms "Falun Gong," "Dalai Lama," or "human rights" would omit hundreds of web pages that were filtered out as a result of the use of such technology.

Jamming of Internet content is a related technique used by repressive governments, including those in Cuba, Belarus, North Korea and elsewhere. China's Golden Shield Project, which the Ministry of Public Security reportedly began operating in 2003, is one of the most sophisticated Internet blocking/jamming programs. It intercepts certain IP addresses and blocks content by preventing offending materials from entering certain IP gateways and proxy servers. Opponents have accused multinational companies, such as Nortel Networks, Cisco and Sun Microsystems, of supporting the Golden Shield Project. Industry representatives counter that the

same technology which fuels the Internet's sharing of information can also be manipulated to facilitate censorship.

The Act does not intend to require American companies to stop conducting business in countries designated as Internet-restricting. Nor does it intend to interfere with legitimate law enforcement operations in those countries. But it is intended to ensure that American companies do more than just consider the jailing of innocent activists who express their political views using the Internet technology provided by American firms as a cost of doing business with these regimes. As a result, the Act establishes procedures to ensure that where an American Internet company receives a law enforcement request from an Internet-restricting government, the request must be conveyed and responded to through the U.S. Department of Justice. In this way, rights to free expression guaranteed by international law will be protected. Even in Internet-restricting countries, law enforcement investigations of terrorism, pornography and other crimes which rely on evidence from the Internet should continue unimpeded as long as the procedures involving the Department of Justice are followed.

HEARINGS

The House International Relations Committee's Subcommittee on Asia and the Pacific and Subcommittee on Africa, Global Human Rights and International Operations held a joint hearing entitled, "The Internet in China: A Tool for Freedom or Oppression?" on February 15, 2006. A subsequent November 6, 2007 hearing focused on Yahoo!'s provision to Congress of false information regarding the Shi Tao case during that previous hearing.

COMMITTEE CONSIDERATION

On October 23, 2007, the Committee held a markup and considered H.R. 275. A motion to report the bill, as amended, to the House, a quorum being present, was agreed to by unanimous consent.

VOTES OF THE COMMITTEE

There were no recorded votes on H.R. 275.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

In compliance with Clause 3(c) (2) of House Rule XIII, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office, pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, November 20, 2007.

Hon. TOM LANTOS, *Chairman,*
Committee on Foreign Affairs,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 275, the Global Online Freedom Act of 2007.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Sunita D'Monte, who can be reached at 226–2840.

Sincerely,

PETER R. ORSZAG.

Enclosure

cc: Honorable Ileana Ros-Lehtinen
Ranking Member

H.R. 275—Global Online Freedom Act of 2007.

H.R. 275 would authorize a new office within the Department of State. The Office of Global Internet Freedom would:

- Coordinate interagency efforts to promote abroad the free flow of electronic information on the Internet,
- Fight efforts by foreign governments to restrict Internet use,
- Identify, update, and publicize a list of key words, terms, and phrases related to human rights, democracy, religious freedom, and political dissent,
- Consult with technology companies, human rights organizations, and academic experts on new information technologies to develop a voluntary code of corporate standards for the free flow of electronic information, and
- Provide pertinent information to the Secretary of State for reports on human rights practices, security assistance, and countries that restrict Internet use.

ESTIMATED COST TO THE FEDERAL GOVERNMENT

Based on information from the department, CBO estimates that the new office would require additional appropriations in 2008 of $2 million for salaries and expenses, $10 million to identify and regularly update key words, and an additional $10 million to develop and implement global strategies and programs to prevent restrictions on Internet use. With annual adjustments for inflation, CBO estimates that activities of the new office would cost $19 million in 2008 and $108 million over the 2008–2012 period, assuming appropriation of the estimated amounts (see table). The costs of this legislation fall within budget function 150 (international affairs).

By Fiscal Year, in Millions of Dollars

	2008	2009	2010	2011	2012
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Estimated Authorization Level	22	22	23	23	24
Estimated Outlays	19	21	22	23	23

Other provisions in the bill would require the Secretary of Commerce to complete a feasibility study on the development of export controls and licenses for items that would allow foreign governments to restrict use of the Internet, and to provide a report to the Congress. CBO estimates those provisions would increase discretionary spending by less than $500,000 a year, assuming the availability of the estimated amounts.

In addition to the discretionary costs, enacting H.R. 275 also could increase collections of civil and criminal fines for violations of the bill's provisions relating to the protection of personally identifiable information. Such fines are recorded in the budget as revenues. CBO expects that any additional collections would not be significant because of the relatively small number of cases likely to be affected. Criminal fines are deposited in the Crime Victims Fund and later spent. CBO expects that any additional direct spending would not be significant.

PRIVATE–SECTOR AND INTERGOVERNMENTAL IMPACT

H.R. 275 would impose private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), on U.S. businesses that host Internet content in foreign countries that are designated as countries that restrict use of the Internet. The bill would prohibit U.S. businesses from cooperating with those foreign governments by blocking certain Web sites and online content and from providing those countries with the personal information of certain Internet users. The bill also would require U.S. businesses in countries that restrict Internet use to provide the Office of Global Internet Freedom with information regarding Web sites and online search engines that are blocked, filtered, or censored in order to comply with the policies or requests of a country that restrict Internet use.

The cost of complying with the mandates would depend in part on which countries are designated by the President under the bill. The cost also would depend on the current practices of U.S. businesses operating in the designated countries and the actions taken by those countries in response to the restrictions placed on such businesses. CBO does not have sufficient information to determine whether the aggregate cost of the mandates in the bill would exceed the annual threshold established in UMRA for private-sector mandates ($131 million in 2007, adjusted annually for inflation).

H.R. 275 contains no intergovernmental mandates as defined in UMRA and would not affect the budgets of state, local, or tribal governments.

STAFF CONTACTS

The CBO contacts for this estimate are Sunita D'Monte (for federal costs), who can be reached at 226–2840, and MarDestinee C. Perez (for private-sector mandates), who can be reached at 226–

2940. This estimate was approved by Peter H. Fontaine, Assistant Director for Budget Analysis.

PERFORMANCE GOALS AND OBJECTIVES

The Act is intended to reduce Internet censorship, to protect personally identifiable information in restricting countries and to highlight the problems caused when the Internet is used as a tool of repression.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d) (1) of rule XIII of the Rules of the House of Representatives, the Committee finds the authority for this legislation in article I, section 8 of the Constitution.

NEW ADVISORY COMMITTEES

H.R. 275 does not establish or authorize any new advisory committees.

CONGRESSIONAL ACCOUNTABILITY ACT

H.R. 275 does not apply to the Legislative Branch.

EARMARK IDENTIFICATION

H.R. 275 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

SECTION-BY-SECTION ANALYSIS AND DISCUSSION

Section 1. Short Title.

This section provides that the short title of the Act is the "Global Online Freedom Act of 2007."

Section 2. Findings.

This section outlines specific findings regarding the power of the Internet to expand information and support freedom when it is not subject to censorship or used as a tool of a police state.

Section 3. Definitions.

This section sets forth definitions necessary to understand the Act's operative provisions. Of particular note, the Act defines the term "personally identifiable information" broadly to include anything that could be used to identify a political dissident or other peaceful user. It also defines the range of United States businesses subject to the Act broadly to include foreign subsidiaries or companies, such as Yahoo China, which benefit from a U.S.-based or U.S.-trademarked brand, even if separate corporate entities have been established for offices operating in an Internet-restricting country.

Section 4. Severability.

This section provides that, if any provision of the Act is found invalid, the remainder of the Act shall continue in full force and effect.

TITLE I—PROMOTION OF GLOBAL INTERNET FREEDOM

Section 101. Statement of Policy.

This section provides that United States foreign policy shall support freedom of expression regardless of the type of media or frontier utilized; that the United States should use all appropriate instruments to support the free flow of information; and that the U.S. should deter American businesses from cooperating with Internet-restricting countries' political censorship.

Section 102. Sense of Congress.

This section provides that the President should urge other countries to promote Internet freedom and the goals of this Act and states that a U.S. business that empowers or assists foreign governments that restrict the Internet are acting contrary to the foreign policy interests of the United States.

Section 103. Annual Country Reports on Human Rights Practices.

This section provides that the State Department's Annual Human Rights Report and related reports concerning economic and security assistance should describe the availability of the Internet, the status of Internet censorship and filtering, and a description of cases in which persons have been jailed or prosecuted for peaceful expression of political, religious or dissenting views on the Internet.

Section 104. Office of Global Internet Freedom.

This section establishes an Office of Global Internet Freedom in the State Department. It provides that this office's duties shall include coordination of interagency efforts to promote on-line freedom, collection of information about Internet censorship and jamming, and support for the President in his designation of Internet-restricting countries. It requires that other Federal department shall cooperate with the Office.

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

This section provides that the President shall annually designate Internet-restricting countries based on an assessment of the government's restriction of Internet freedom during the preceding year. A report identifying the designated countries should be transmitted to Congress within 180 days of enactment of the Act and then annually thereafter.

TITLE II—MINIMUM CORPORATE STANDARDS FOR ONLINE FREEDOM

Section 201. Protection of Personally Identifiable Information.

This section contains two subsections related to the protection of personally identifiable information. Subsection (a) forbids U.S. businesses from locating within Internet-restricting countries electronic communication that contain personally identifiable information. Storage of such communications must be done within the United States or overseas in countries that are not designated Internet-restricting. Subsection (b) establishes definitions related to this provision.

Section 202. Integrity of Personally Identifiable Information.

This section provides that, where a U.S. business collects or obtains personally identifiable information through provision of services or products on the Internet, the business may not provide that information to the Internet-restricting country. In noting that the information may not be provided to officials of the Internet-restricting country, the Act intends that no government official, including those with police or security functions, may have access to the information in any way, except through the legitimate law enforcement channels established by the Department of Justice. The purpose of this subsection is to change the dynamics of the quest for information by law enforcement agencies of Internet-restricting countries. Rather than approaching the American businesses directly, the Act changes the dynamic involved with seeking such information into a government-to-government request. This is aimed to minimize direct and indirect pressure on American businesses. The Department of Justice, not the American business or the requesting law enforcement agency, should be the arbiter of whether the request is for a legitimate law enforcement purpose. Subsection (c) provides than anyone aggrieved by a violation of this section shall enjoy a private right of action for damages, including compensatory and punitive damages, in the United States. This section is intended to allow a right of action for American citizens and non-Americans who fall within the jurisdiction of U.S. courts, including the family members of those jailed overseas in connections with actions by U.S. companies.

Section 203. Transparency Regarding Search Engine Filtering.

This section provides that U.S. businesses that operate Internet search engines must provide to the State Department Office of Global Internet Freedom information about any policies or search terms used by an Internet-restricting country for Internet and search engine censorship.

Section 204. Transparency Regarding Internet Censorship.

This section provides that U.S. businesses that operate Internet content hosting services must provide to the State Department Office of Global Internet Freedom information about any policies, categories or specific Uniform Resource Locators (URLs) used by an Internet-restricting country for Internet and search engine censorship.

Section 205. Protection of United States-Supported On-Line Content.

This section provides that U.S. businesses may not conduct Internet jamming of U.S.-supported Web sites or U.S. supported Internet content in designated countries.

Section 206. Penalties.

This section provides civil and criminal penalties of a maximum of $2 million for violations of the Act.

Section 207. Presidential Waiver.

This Section provides the President may waive application of sanctions if he deems that the country has ceased the activities

leading to its designation, the waiver would advance global Internet freedom or the waiver is in the Interests of national security.

TITLE III—EXPORT CONTROLS FOR INTERNET–RESTRICTING COUNTRIES

Section 301. Feasibility Study on Establishment of Export Controls.

The Act requires that a feasibility study shall be conducted regarding development of export license requirements to end users in Internet-restricting countries for purposes of restricting Internet freedom. The study shall consider and advise how export controls with end-user restrictions could be established concerning, but not limited to: (i) software used to censor the Internet or to identify key terms for the purposes of restricting Internet communications; (ii) routers, filters and other hardware used to censor the Internet or to identify key terms for purposes of restricting Internet communications; and (iii) the deemed export of personally identifiable information collected or controlled by Internet companies that could be used to identify political dissidents or to otherwise restrict Internet communications. Such a study should build on the work of government, industry and non-government representatives.

Section 302. Report.

This section provides that the Secretary of Commerce shall issue a report of the feasibility study within 180 days of the Act's enactment.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italics and existing law in which no change is proposed is shown in roman):

FOREIGN ASSISTANCE ACT OF 1961

PART I

CHAPTER 1—POLICY; DEVELOPMENT ASSISTANCE AUTHORIZATIONS

* * * * * * *

SEC. 116. HUMAN RIGHTS.—(a) * * *

* * * * * * *

(g)(1) The report required by subsection (d) shall include an assessment of the freedom of electronic information in each foreign country. Such assessment shall include the following:

(A) An assessment of the general extent to which Internet access is available to and used by citizens in that country.

(B) An assessment of the extent to which government authorities in that country attempt to filter, censor, or otherwise block Internet content, as well as a description of the means by which they attempt to block such content.

(C) A description of known instances in which government authorities in that country have persecuted, prosecuted, or oth-

erwise punished a person or group for the peaceful expression of political, religious, or dissenting views via the Internet, including electronic mail.

(D) A description of known instances in which government authorities in that country have sought to collect, request, obtain or disclose the personally identifiable information of a person in connection with that person's communication of ideas, facts or views where such communication would be protected by the International Covenant on Civil and Political Rights.

(2) In compiling data and making assessments for the purposes of paragraph (1), United States diplomatic mission personnel shall consult with human rights organizations, technology and internet companies and other appropriate nongovernmental organizations.

* * * * * * *

PART II

CHAPTER 1—POLICY

* * * * * * *

SEC. 502B. HUMAN RIGHTS.—(a) * * *

* * * * * * *

(i)(1) The report required by subsection (b) shall include an assessment of the freedom of electronic information in each foreign country. Such assessment shall include the following:

(A) An assessment of the general extent to which Internet access is available to and used by citizens in that country.

(B) An assessment of the extent to which government authorities in that country attempt to filter, censor, or otherwise block Internet content, as well as a description of the means by which they attempt to block such content.

(C) A description of known instances in which government authorities in that country have persecuted, prosecuted, or otherwise punished a person or group for the peaceful expression of political, religious, or dissenting views via the Internet, including electronic mail.

(D) A description of known instances in which government authorities in that country have sought to collect, request, obtain or disclose the personally identifiable information of a person in connection with that person's communication of ideas, facts or views where such communication would be protected by the International Covenant on Civil and Political Rights.

(2) In compiling data and making assessments for the purposes of paragraph (1), United States diplomatic mission personnel shall consult with human rights organizations, technology and internet companies, and other appropriate nongovernmental organizations.

* * * * * * *

○