Increasing Global Demand for an Uncensored Internet—How the U.S. Can Help Defeat Online Censorship by Facilitating Private Action

ABSTRACT

This Note discusses efforts to defeat government censorship of the Internet. In the narrow meaning of that idea, this Note initially discusses technological efforts to circumvent government-imposed Internet firewalls; in the broader sense, it addresses the larger goal of inducing censoring governments to bring their firewalls down. Proposed U.S. legislation would provide U.S. government funding of censorship circumvention technology. This Note discusses why such funding is not a good approach. Absent larger international efforts, private action—within both the U.S. and censoring countries—has the best chance of bringing down government-run firewalls. This Note discusses how the U.S. government can best facilitate such private action through a two-pronged approach. The approach attempts to increase private circumvention efforts while decreasing U.S. corporate assistance in foreign governments' censoring. This Note argues that such an approach would result in the possibility of censoring governments bringing down their firewalls because of an increased demand for an uncensored Internet and sufficient government frustration in maintaining such censorship.

TABLE OF CONTENTS

I. INTRODUCTION

The Global Internet Freedom Act of 2006[1] and the Global Online Freedom Act of 2007[2] propose government funding of "anti-jamming" technology that allows users in Internet-censoring countries to view

1. Global Internet Freedom Act, H.R. 4741, 109th Cong. (2006).
2. Global Online Freedom Act, H.R. 275, 110th Cong. (2007).

websites that are blocked by their government.[3] U.S. government funding of such technology is not a good long-term approach to defeating government Internet censorship. The U.S. government would be perceived internationally as imposing its own standards of decency and morals onto China and other countries with similar Internet censorship. Such criticism gains legitimacy when it is viewed in light of the U.S. government's own restrictions on Internet freedom regarding suspected terrorism, pornography, and content deemed obscene.[4]

The U.S. government does not permit a completely free Internet within its own borders, yet would be actively supplanting other countries' content restrictions under the proposed legislation.[5] Government funding of such technology contradicts the spirit of U.S. courts' own community standards test, which allows the most restrictive standard within the U.S. to govern what is decent online.[6] Funding of technology that circumvents foreign censorship amounts to a statement that while the most restrictive standard in the U.S. is an important consideration, the most restrictive standards abroad must be torn down. Given that the U.S. has included its own content filters in such software offerings in the past,[7] the U.S. would essentially be replacing another government's firewall with its own.

This Note proposes that the U.S. government should not fund anti-jamming software, but should rather take an approach that would better facilitate private action to defeat Internet censorship. This suggested approach includes (1) allowing anonymization websites that are aimed at circumventing government censorship to operate with minimal U.S government involvement, and (2) attempting to minimize U.S. corporate assistance in foreign governments' censorship efforts. This Note will discuss the history of Internet censorship in China and other censoring countries, critically analyze the Global Internet Freedom Act and Global Online Freedom Act, outline a better approach, and discuss how the advocated approach would promote breaking government-imposed firewalls from within Internet-censoring countries.

---

3. The Global Internet Freedom Act explicitly calls for government funding of anti-jamming software, while the Global Online Freedom Act simply implies that such funding is likely. *See infra* Part III.B.

4. *See infra* Part III.D-E.

5. *See infra* Part III.D.

6. *See infra* Part III.E.

7. *See infra* Part III.D.

II. BACKGROUND INFORMATION

A. *An Overview of Censorship Methods*

The 2002 House policy statement supporting the original Global Internet Freedom Act, entitled "Tear Down This Firewall," states that the "most notorious violators of Internet freedom" are Cuba, Laos, North Korea, China, Saudi Arabia, Syria, Tunisia, and Vietnam.[8] According to the report, which cites the Human Rights Watch and Reporters Without Borders, the control methods used by these governments include "denying their citizens access to the Internet, censoring content, banning private ownership of computers, and even making e-mail accounts so expensive that ordinary people cannot use them."[9] The blocking and censoring methods are most often in the form of government-run firewalls and filters.[10] Some governments also monitor individual activity, for example, screening for certain words in emails or message boards, and may "black list" individual users or even prosecute them.[11]

For those countries where the Internet is at least somewhat accessible, the most widely used method of government interference with Internet access is content censorship.[12] Content censorship is also the method most easily defeated from abroad through the technologies discussed in this Note. As will be discussed, as long as a censored country's citizens have partial Internet access, it is possible to base technology outside of the firewall or filter (abroad) that will open up more (or all) of the Internet to users that connect to Internet content through such foreign-run websites or programs.

Censorship is most commonly accomplished by means of proxy servers that are interposed between the end user and the Internet. This form of censorship is most easily implemented when the government acts as the Internet Service Provider (ISP).[13] It requires, at a minimum, that the government have control over the country's ISPs.[14] While the House policy statement states that the "strictest enforcers of Internet censorship are Bahrain, China, Iran, Kuwait, Saudi Arabia, Vietnam, and Yemen,"[15] this Note will focus mostly on

---

8. HOUSE POLICY COMMITTEE, POLICY STATEMENT, ESTABLISHING GLOBAL INTERNET FREEDOM: TEAR DOWN THIS FIREWALL (2002),, *available at* http://web.archive.org/web/20021014010556/http://policy.house.gov/html/news_item.cfm?id=112 [hereinafter TEAR DOWN THIS FIREWALL].

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.*

13. *Id.*

14. *Id.*

15. *Id.*

China. This Note's focus on China is in line with a similar focus by both the Global Internet Freedom Act[16] and the most prominent private anti-jamming technologies.[17]

Chinese regulation of the Internet has become increasingly strict since the Internet began.[18] One of the first laws came through the "PRC [People's Republic of China] Interim Provisions of the Regulation of Computer Networks and the Internet" in 1995.[19] These provisions' basic message was that existing state laws apply on the Internet.[20] The interim provisions were superseded by the "PRC Measures on the Regulations of Public Computer Networks and the Internet" in April 1996.[21] These provisions were more expansive and tailored to the Internet, prohibiting activities like hacking and computer viruses.[22] The provisions also began the Chinese government's heavy reliance on self-censorship and self-regulation by stating that citizens must report criminal activity and must cooperate with government monitoring and inspection.[23]

In 2002, the Chinese government added to its censorship arsenal by implementing software filtering based on keywords.[24] This software blocks certain portions of sites that are not initially blocked by the firewall, resulting in additional access to some previously blocked websites.[25] However, it had the negative effect of filtering email by keyword, which was not censored as strongly before.[26]

The Chinese government has arrested dozens of its citizens for their political speech on the Internet.[27] The government has also arrested Chinese citizens who have published newsletters promoting freedom of information on the Internet.[28] Lin Hai testified at a Congressional roundtable regarding his need to leave China for the U.S. in order to continue his efforts to promote free speech after being imprisoned for 18 months as a result of his newsletter, which

---

16. *See id.* (stating that China "commits the most Internet abuses" and retains control over 33.7 million Internet users).

17. *See infra* Part II.A, II.B.

18. Phil Deans, *The Internet in the People's Republic of China: Censorship and Participation*, *in* THE POLITICAL ECONOMY OF THE INTERNET IN ASIA AND THE PACIFIC 122, 122 (Jason P. Abbott ed., 2004).

19. *Id.* at 128.

20. *Id.*

21. *Id.*

22. *Id.*

23. *Id.* at 128-29.

24. Jill R. Newbold, Note, *Aiding the Enemy: Imposing Liability on U.S. Corporations for Selling China Internet Tools to Restrict Human Rights*, 2003 U. ILL. J.L. TECH. & POL'Y 503, 511 (2003).

25. *Id.*

26. *Id.* at 512.

27. *Id.* at 508.

28. *China's Cyber-Wall: Can Technology Break Through?: Roundtable Before the Cong.-Exec. Commission on China*, 107th Cong. 8 (2002) (statement of Lin Hai Computer Scientist, Shanghai, China).

promoted such ideas.[29] Once in the United States, he worked on software aimed at circumventing Chinese censorship of email.[30] Because the Chinese government often blocks email subscription lists from Voice of America, Radio Free Asia, and other organizations distributing information about ways around Chinese firewalls, providing the Chinese people with access to uncensored email ties into the larger goal of access to an uncensored Internet.[31]

Lin Hai's frustration in promoting freedom of speech from within China is an example—particularly given his relative success after moving to the U.S.—that individuals outside of China must be involved in such efforts. His story also hints that the Chinese government is not immune to buckling under pressure for change, both from within China and abroad. Lin Hai's time in jail was shortened due to the attention given to the matter by the media and outside human-rights organizations.[32] This lends additional credence to an idea put forth by Bill Xia: "[T]echnology alone will not decide the future of China's cyber-wall, but people do. If all Chinese people would like to obtain uncensored information, the cyber-wall will be broken from the inside."[33]

The Lin Hai story suggests that the Chinese government will go after citizens who attempt to spread the word of anti-censorship technology. The more important question for Internet freedom in China is to what extent the government will pursue mere users of such technology. Under the "Measures for Managing Internet Information Services," made law in 2000, ISPs are required to record every website a subscriber visits, along with the telephone number used for access.[34] ISPs must maintain records for sixty days and submit them to the government on demand.[35] Thus, the Chinese government could at the very least look back at records once the URL becomes known by the authorities to learn which citizens are accessing the internationally-run sites that allow firewall circumvention. This threat is obviously even greater in other countries where ISPs are under the monopoly control of the government through state control of the telecommunications systems.[36]

---

29. *Id.*
30. *Id.*
31. *Id.* at 9.
32. *Id.* at 8.
33. *Id.* at 7 (statement of Bill Xia, President, Dynamic Internet Technology, Inc.).
34. Newbold, *supra* note 25, at 509.
35. *Id.*
36. *See* Philip J. Oliveri, *Technology Software that Counters Internet Jamming: Its Role in the U.S. and in Non-Democratic Countries*, 2003 SYRACUSE L. & TECH. J. 5 (2003) (discussing the ways in which authoritarian governments interfere with and restrict internet access).

China's censorship technology is only part of its formula for content control on the Internet; as mentioned previously, the government also relies heavily on self-censorship resulting from the public's fear of possible punishment.[37] Other countries use more direct, forceful methods of censorship. In Cuba, Fidel Castro only allows Internet access through government-approved institutions,[38] places high taxes on email accounts,[39] and banned the sale of personal computers to the general public in 2002.[40] The Internet essentially does not exist in North Korea because Kim Jong-Il has banned access to any websites outside of the country.[41]

Reporters Without Borders calls North Korea "by far the worst Internet black hole."[42] The computers available to some students and researchers at universities in North Korea are only connected to each other through what is essentially a countrywide intranet.[43] The government monitors this intranet.[44] According to the *New York Times*, "[a] handful of elites have access to the wider Web—via a pipeline through China—but this is almost certainly filtered, monitored and logged."[45] Such use by one country's citizens of another country's less strict Internet regulations will be seen in this Note as the typical method around government firewalls and censorship.

B. *Technologies Used to Circumvent Censorship*

The U.S. has directly funded some anti-jamming technology, but the funding has been limited and targeted specifically at China.[46] According to the text of the Global Internet Freedom Act:

> The United States has thus far commenced only modest steps to fund and deploy technologies to defeat Internet jamming. To date, for example, the Voice of America and Radio Free Asia have committed a total of $3,000,000 for technology to counter Internet jamming of their websites by the People's Republic of China. This technology has been relied upon by Voice of America and Radio Free Asia to ensure access to their programming, and it has successfully permitted 100,000 electronic hits per day from users in China.[47]

---

37. Deans, *supra* note 19, at 122.
38. Oliveri, *supra* note 38, at 6.
39. *Id.* at 8.
40. *Id.* at 7.
41. *Id.* at 7
42. Tom Zeller, Jr., *The Internet Black Hole That Is North Korea*, N.Y. TIMES, Oct. 23, 2006, at C3.
43. *Id.*
44. *Id.*
45. *Id.*
46. *See* Global Internet Freedom Act, H.R. 4741, 109th Cong. § 2 (2006).
47. *Id.*

For the most part, non-governmental organizations and individuals—many of them Chinese dissidents—have been responsible for the creation and costs of anti-jamming software.[48] The techniques have included various technological approaches, including use of proxy servers, intermediaries, mirrored sites, and encryption.[49] A proxy server is a computer that allows indirect connections to other sites by taking the request, accessing the file from the actual location, and then returning it to the user.[50] A mirror site is a website that hosts content that is identical to that at another location; it allows pages to be viewed without ever requesting data from the original server.[51]

1. Examples of Anti-Jamming Software

"Triangle Boy," an anti-jamming technology developed by SafeWeb that allowed Internet access through an encrypted channel, was receiving millions of hits per month from China and Saudi Arabia before closing due to lack of funding.[52] SafeWeb operated public proxy servers that allowed users behind firewalls to access blocked sites.[53] Triangle Boy was a separate software that "spoofed" Internet protocol (IP) addresses and helped users connect to SafeWeb who were unable to access the SafeWeb servers directly (such as users in China).[54] Triangle Boy was a peer-to-peer network by which a user behind a firewall would send a request to a second user, who in turn would connect directly with the SafeWeb server and return the information to the original requester.[55] A peer-to-peer arrangement means that the more "installations" or hosts there are taking requests, the harder it is for a business or country running a firewall to block requests simply by IP address.[56]

"Peekabooty" is a program employing a different approach to defeat Internet jamming.[57] Peekabooty is essentially a peer-to-peer network. When a user wants to access a blocked website, the

---

48. Elaine M. Chen, *Legislative Update - Global Internet Freedom: Can Censorship and Freedom Coexist?*, 13 DEPAUL-LCA J. ART & ENT. L. & POL'Y 229, 242 (2003).

49. *Id.*

50. PC Magazine Encyclopedia, Proxy Server Definition, http://www.pcmag.com/encyclopedia_term/0,2542,t=proxy+server&i=49892,00.asp (last visited Nov. 5, 2007).

51. PC Magazine Encyclopedia, Mirror Site Definition, http://www.pcmag.com/encyclopedia_term/0,2542,t=mirror+site&i=47085,00.asp (last visited Nov. 5, 2007).

52. Chen, *supra* note 49.

53. Steven Bonisteel, *Voice Of America Aims to Break China's Web Site Blockades*, NEWSBYTES NEWS NETWORK, Aug. 30, 2001.

54. *Id.*

55. *Id.*

56. *Id.*

57. Chen, *supra* note 49, at 243.

program uses another computer on the Peekabooty network to access the website and return an encrypted version to the initial requestor.[58] There are also more typical peer-to-peer networks for downloading uncensored content in China, such as Freenet-China.[59] Many variations of the peer-to-peer structure have emerged recently, such as Psiphon and Tor.[60] The technological differences between such offerings aren't particularly relevant to this Note, but the growing array of anti-jamming options is.

"Anonymizer," a for-profit website that allows anonymous Internet browsing (primarily targeted not at overcoming censorship, but providing privacy to users in non-censoring countries) has entered the arena of anti-jamming technology.[61] Its "Operation: Anti-Censorship" project is currently free.[62] The company has been actively monitoring the amount of time it takes for the Chinese government to block the site, finding that the time period is usually more than a week.[63] When this occurs, the service simply sets up under a new address, but the company claims that it has "other tricks up its sleeve" if the government becomes quicker at blocking sites.[64] The company claims that it is willing to update on a daily basis and to employ additional technology that would make it more difficult for the Chinese government to identify and block the site.[65] The project is currently online for Chinese citizens and a version is under development for users in Iran.[66]

2. Recent Private Collaborative Efforts

In December 2006, four of the largest companies in Internet anti-jamming technologies reached an agreement to fully cooperate in their technology and business operations.[67] The four companies are: World's Gate, Inc.; Dynamic Internet Technology, Inc.; the UltraReach Internet Corp.; and Garden Networks for Freedom of

---

58. *Id.*
59. *Id.*
60. *See* Hiawatha Bray, *Beating Censorship on the Internet*, BOSTON GLOBE, Feb. 20, 2006 (discussing Psiphon and Tor).
61. *See* Sumner Lemon, *Anonymizer Prepares to Battle China's Net Censors*, INFOWORLD, Apr. 4, 2006, http://www.infoworld.com/article/06/04/04/77090_HNanonymizer prepares_1.html (discussing Anonymizer's product).
62. *Id.*
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.*
67. *Internet Anti-Jamming Technology Companies Reach Milestone Agreement*, RED ORBIT, Dec. 18, 2006, http://www.redorbit.com/news/technology/772439/internet_ antijamming_technology_companies_reach_milestone_agreement/index.html?source=r_ technology [hereinafter *Milestone Agreement*].

Information.[68] The total number of visits to these companies' sites has exceeded one billion.[69] Bill Xia is the president of the Dynamic Internet Technology.[70] He said that the "[f]unding of these anti-blockade tools and services, in addition to the income from various service contracts, comes from donations and in-kind contributions in different forms from people from all walks of life."[71] He added that many of the employees of these companies work on a volunteer basis.[72]

In order to help operate with limited funding, these companies are now hoping that websites profiting from the new Chinese audience that anti-jamming technology creates will contribute to the cost.[73] Although acknowledging the increasing costs of maintaining free services, the companies believe that they will continue to find funding in order to operate as long as such services are needed.[74] Alex Wang, vice president of World Gate, maintains that his company "will continue [its] efforts until the information censorship inside China completely ceases."[75] While China, as usual, is the main focus of such software, the software also has users in Belarus, Cuba, Ethiopia, Iran, Laos, North Korea, Tunisia, and Vietnam.[76]

C. *The Global Internet Freedom Act of 2006 (GIFA)*

The Global Internet Freedom Act (GIFA), most recently introduced on February 14, 2006, failed to make it out of the House Committee on International Relations.[77] Versions of GIFA have been submitted to three sessions of Congress.[78] While it has not been introduced in the current session, GIFA continues to warrant discussion for its frequently cited supporting policy statement,[79] and as a prominent example of the viewpoint that the U.S government should fund anti-jamming software.

The official stated purpose of GIFA is "[t]o develop and deploy technologies to defeat Internet jamming."[80] GIFA defines Internet jamming as "jamming, censoring, blocking, monitoring, or restricting

---

68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*
72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.*
77. Global Internet Freedom Act, H.R. 4741, 109th Cong. (2006).
78. *See* GovTrack.us, H.R. 4741 [109th]: Global Internet Freedom Act, http://www.govtrack.us/congress/bill.xpd?bill=h109-4741 (last visited Nov. 4, 2007) (setting forth the history of H.R. 4741).
79. TEAR DOWN THIS FIREWALL, *supra* note 9.
80. H.R. 4741.

Internet access and content by using technologies such as firewalls, filters, and 'black boxes.'"[81] GIFA is presumably applicable to all countries involved in Internet jamming, but specifically lists Burma, Cuba, Iran, Laos, the Maldives, North Korea, China, Saudi Arabia, Syria, and Vietnam.[82] The First Amendment and Article 19 of the United Nations' Universal Declaration of Human Rights are cited for support of the policy behind the bill.

The goals of GIFA include establishing an office within the International Broadcasting Bureau devoted to countering Internet jamming and expediting the development and deployment of anti-jamming technology, including funding of development in the private sector.[83] GIFA would create the Office of Global Internet Freedom within the International Broadcasting Bureau, which would be responsible for developing a "comprehensive global strategy to combat state-sponsored and state-directed Internet jamming."[84] The Office would receive appropriations of $50,000,000 per year for 2007 and 2008.[85]

As discussed previously, the 2002 House policy statement entitled "Tear Down This Firewall" outlines more detailed goals for the bill.[86] The statement emphasizes the need for government utilization of the technologies already in use in the private sector to promote "global Internet freedom."[87] It also calls for a resolution at the U.N. Human Rights Commission's annual meeting "condemning all nations practicing Internet censorship and denying freedom to access information."[88]

D. *The Global Internet Freedom Task Force (GIFT)*

Secretary of State Condoleezza Rice established the Global Internet Freedom Task Force (GIFT) on February 14, 2006.[89] GIFT was established as "an internal State Department coordination group to address challenges to freedom of expression and the free flow of information on the Internet."[90] GIFT aims "to maximize freedom of expression and the free flow of information and ideas, to minimize the success of repressive regimes in censoring and silencing legitimate debate, and to promote access to information and ideas over the

---

81. *Id.* § 6.
82. *Id.* § 2.
83. *Id.* § 3.
84. *Id.* § 4.
85. *Id.*
86. TEAR DOWN THIS FIREWALL, *supra* note 9.
87. *Id.*
88. *Id.*
89. U.S. DEP'T OF STATE, STATE SUMMARY OF GLOBAL INTERNET FREEDOM TASK FORCE, FACT SHEET (2006) [hereinafter FACT SHEET].
90. *Id.*

Internet."[91] The GIFT strategy has three priorities: (1) monitoring Internet freedom in countries around the world; (2) responding to challenges to Internet freedom; and (3) advancing Internet freedom by expanding Internet access.[92]

GIFT outlines the methods it plans to employ to achieve each of the three priorities mentioned above.[93] The "monitoring" priority is to be achieved by expanded monitoring and reporting of abuses of freedom of expression.[94] This information will be included in an annual human rights report.[95] GIFT also plans to increase interim embassy reporting of Internet freedom violations.[96]

The "responding" priority is more passive than the title would suggest. GIFT plans to achieve this priority by raising awareness and working with international organizations.[97] The protests will be directed to the foreign governments practicing Internet repression.[98] GIFT plans to press the Internet freedom issue in meetings with foreign officials.[99] It also claims to "stand ready to engage appropriately with the technology industry, non-governmental organizations (NGOs), and other stakeholders in a process aimed at developing shared principles to guide private sector activities in restrictive economies."[100]

Under the "advancing" priority, the GIFT fact sheet essentially outlines pre-existing government funds and projects supporting Internet freedom causes that it expects to continue.[101] The fact sheet mentions both government programs (USAID and the Telecommunications Leadership Program) and public-private partnerships (the Digital Freedom Initiative) that have helped to expand Internet access in developing countries.[102] The fact sheet also includes the announcement by the State Department's Bureau for Democracy, Human Rights, and Labor of a $500,000 grant program "for innovative proposals and cutting-edge approaches to combat Internet censorship in countries seeking to restrict basic human rights, including freedom of expression."[103]

As a basis for the establishment of GIFT, the fact sheet states that "freedom of expression is a universal right."[104] GIFT cites in

---

91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. *Id.*
96. *Id.*
97. *Id.*
98. *Id.*
99. *Id.*
100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.*

support of this statement both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[105] GIFT claims that international law allows limited restrictions on speech for "legitimate government purposes" such as "national security" and "public order."[106] However, "repressive regimes misuse such exceptions as a pretext to censor speech about democracy and human rights and suppress dissent."[107]

E. *The Role of U.S. Corporations in China's Internet Censorship*

On August 1, 2002, the Chinese government enacted legislation requiring ISPs to self-censor their websites.[108] If an ISP does not comply, the government may shut down the websites.[109] Before the legislation was enacted, many businesses and other organizations signed a voluntary, government-sponsored "Public Pledge on Self-Discipline for the China Internet Industry."[110] This list included some Western corporations, including Yahoo!.[111] The pledge stated in part that "[s]ignatories agree to refrain from producing, posting or disseminating harmful information that may jeopardize state security and disrupt social stability."[112]

The U.S. companies that signed the pledge or otherwise censor versions of their sites specifically for China are spending hundreds of millions of dollars on such censorship through personnel training and the purchasing and maintenance of equipment.[113] Complying with China's censorship standards also presents practical difficulties for a search engine, as the Chinese government will not give companies a list of the government's blocked sites or keywords.[114] In order to create the self-censored Google.cn search engine, Google set up computers inside China to access international sites, one after another, adding blocked sites to the search engine's own blacklist.[115] The costs incurred by self-censoring ISPs and websites in efforts to

---

105. *Id.*
106. *Id.*
107. *Id.*
108. Newbold, *supra* note 25, at 510.
109. *Id.*
110. *Id.*
111. *Id.* at 510, 513.
112. *Id.* at 510.
113. *Id.* at 513.
114. *See* Clive Thompson, *Google's China Problem (and China's Google Problem)*, N.Y. TIMES MAGAZINE, Apr. 23, 2006 (discussing Google's difficulties in the Chinese Market).
115. *Id.* While Google mirrors the Chinese government's blacklist in Google.cn, Google decided to continue offering Chinese users the old Google.com as well, which "would produce uncensored search results, though controversial links would still lead to dead ends, and the site would be slowed down and occasionally blocked entirely by the firewall." *Id.*

comply with China's censorship laws allow the Chinese government to save money and resources that would otherwise be devoted to developing censorship methods and policing these sites.[116]

U.S. companies also provide China with various pieces of its Internet filtering software: "Cisco's firewalls help the Chinese government monitor email; Microsoft proxy servers block Web pages; Nortel aids the Chinese government in tracking its citizens' surfing habits; and Websense contributes sophisticated filtering and monitoring techniques."[117] Yahoo! has even given the Chinese government personal information about alleged dissidents.[118]

On February 15, 2006, Google, Microsoft, Yahoo!, and Cisco were called in a Congressional hearing for aiding and abetting the Chinese government's censorship efforts.[119] House members described these corporations' behavior in China as "abhorrent"[120] and "astonishing."[121] The corporations generally responded to the accusations by stating that they believed the benefits of their actions towards freedom of expression in the long term outweighed the downsides.[122]

Yahoo! and Google each explicitly asked the government for help in fighting Chinese censorship.[123] Google, for instance, "urged the State Department and the U.S. trade representative to press U.S. concerns on censorship during talks with foreign governments."[124] The companies involved in the hearing seemed to welcome U.S. legislation that could provide U.S. companies with an excuse to give the Chinese government for not complying with China's censorship laws.[125] Andrew McLaughlin, Google's senior policy counsel, even

---

116. Newbold, *supra* note 25, at 512-13.

117. *Id.* at 513.

118. Marc Gunther, *Yahoo's China Problem*, FORTUNE, Feb. 22, 2006, *available at* http://money.cnn.com/2006/02/21/news/international/pluggedin_fortune/.

119. *Tech Giants Defend Actions in China - Lawmakers Blast Companies as Collaborators in Suppressing Dissent*, ASSOCIATED PRESS, Feb. 15, 2006, *available at* http://www.msnbc.msn.com/id/11347853/.

120. *Id.* ("'Your abhorrent actions in China are a disgrace,' said Rep. Tom Lantos, the top Democrat on the House International Relations Committee. 'I simply don't understand how your corporate leadership sleeps at night.'").

121. *Id.* ("Rep. Jim Leach, R-Iowa, said Google seemingly had acted 'as a functionary of the Chinese government. . . . This is astonishing.'").

122. *Id.* ("Microsoft's associate general counsel, Jack Krumholtz, said his company was committed to staying in China because of the Internet's potential for eventually allowing free access to information. 'We think the benefits far outweigh the downside, in terms of promoting freedom of expression,' he said.").

123. *Id.*

124. *Id.*

125. *Id.*

suggested that "[c]ensorship should be treated as a trade barrier and be written into free-trade agreements."[126]

F. *The Global Online Freedom Act of 2007 (GOFA)*

The Global Online Freedom Act (GOFA), after failing to become law in 2006, was re-introduced on January 5, 2007.[127] The bill aims to "promote freedom of expression on the Internet" and "to protect United States businesses from coercion to participate in repression by authoritarian foreign governments."[128] In addition to findings similar to those previously listed in GIFA and the associated policy statement, the bill includes the finding that China's censorship "promotes, perpetuates, and exacerbates a xenophobic—and at times particularly anti-American—Chinese nationalism, the long-term effect of which will be deleterious to United States efforts to prevent the relationship between the United States and China from becoming hostile."[129] The bill calls for a U.S. policy of using "diplomacy, trade policy, and export controls" to promote the free flow of information on the Internet, and deterring U.S. businesses from "cooperating with officials of Internet-restricting countries in effecting the political censorship of online content."[130]

GOFA would establish the Office of Global Internet Freedom in the Department of State.[131] The Office would be appropriated fifty million dollars for each of the fiscal years 2008 and 2009.[132] The duties funded would include the duty to "develop and ensure the implementation of a global strategy and programs to combat state-sponsored and state-directed Internet jamming by authoritarian foreign governments."[133] The Office would consult with technology companies, human rights organizations, and academic experts in order to establish "a voluntary code of minimum corporate standards related to Internet freedom."[134]

GOFA would not allow any U.S. business to locate "any electronic communication that contains any personally identifiable information" within an Internet-restricting country, as designated by

---

126. Anne Broache, *Web Giants Ask for Feds' Help on Censorship*, CNET NEWS, Jan. 30, 2007, *available at* http://news.com.com/Web+giants+ask+for+feds+help+on+censorship/2100-1028_3-6154930.html.

127. Global Online Freedom Act, H.R. 275, 110th Cong. (2007); Global Online Freedom Act, H.R. 4780, 109th Cong. (2006).

128. H.R. 275.

129. *Id.* § 2(12).

130. *Id.* § 101.

131. *Id.* § 104(a).

132. *Id.* § 104(e).

133. *Id.* § 104(b).

134. *Id.*

the President.[135] A private right of action would be created against any U.S. business that provides personally identifiable information to an official of an Internet-restricting country, unless the information was provided for legitimate foreign law-enforcement purposes as determined by the Department of Justice.[136] GOFA would call for increased transparency regarding search engine filtering, requiring search engine companies to provide the Office with a list of filter terms used to comply with foreign censorship practices.[137] Internet content hosting services would be required to provide similar lists of URLs that they have removed or blocked due to foreign censorship practices.[138] GOFA also calls for a feasibility study on the establishment of export license requirements for technology that facilitates restrictions on Internet freedom.[139]

III. ANALYSIS

A. *Is Anti-Jamming Software a Good Approach to Defeat Censorship?*

The question of whether the U.S. should fund anti-jamming software initially requires a decision about whether even privately funded anti-jamming technology is a worthwhile effort. The operation of servers that support anti-jamming technology, as discussed above, has varying costs, depending on the nature of the technology used. The more a system can act as a true peer-to-peer network, the more the costs, largely consisting of the Internet bandwidth use, can be distributed to the volunteering general public of host users in non-censoring countries. If two systems had the same amount of page requests from censored users, a peer-to-peer system like Peekabooty would require less explicit operation funding than a system like Anonymizer, which uses central servers with company-funded bandwidth. This assumes that enough members of the non-censored public are willing to serve as host users to fulfill all the incoming page requests; otherwise, the service would either not fully function or require the overflow to be handled by company-funded bandwidth.

Due to the varying operating costs of anti-jamming software and the constantly changing technology, it is difficult to do any sort of general cost-benefit analysis. It would be possible to determine costs of specific programs, but quantifying the corresponding benefit would be too speculative. To say that the benefit is confined to the actual

---

135. *Id.* § 201(a).
136. *Id.* § 202.
137. *Id.* § 203.
138. *Id.* § 204.
139. *Id.* § 301.

users' downloads and page views is likely shortsighted in ignoring the possible further spread of the ideas read about on the websites viewed. A possible effect down the line, though tenuous, might be that a censoring government feels enough pressure from such programs—from both domestic demand for the uncensored content and the government's own frustrations in blocking the technology—that it takes its firewall down. This Note will discuss that possibility further below.

B. *Government Funding of Anti-Jamming Technology under GIFA and GOFA*

GIFT was established on February 14, 2006,[140] the same day that GIFA was referred to the House Committee on International Relations.[141] Both rely on the same basic premise and background: that the U.S. government should have some additional involvement in the efforts to defeat Internet censorship. Of course, the striking difference between GIFA and GIFT is that GIFA would appropriate $50,000,000 per fiscal year to its established office.[142] Based on the title of the section that includes the appropriations of funds language, GIFA could be interpreted as stating that this money would go specifically to develop and deploy anti-jamming technologies.[143] However, the subsection itself simply reads that the money is "to be appropriated to the Office," with no further qualification on the use of the funds.[144] Based on GIFA's various broad goals, an attempt "to bring to bear the pressure of the free world on repressive foreign governments,"[145] it is possible that this appropriation could be used in efforts that only peripherally touch upon Internet jamming.

GOFA's language appropriating funds is also vague.[146] GOFA is not as explicit as GIFA in regards to funding anti-jamming technologies. Whereas GIFA's established office would be responsible for the "development and deployment of technologies to defeat Internet jamming,"[147] GOFA calls for its established office to "develop and ensure the implementation of a global strategy and programs to

---

140. FACT SHEET, *supra* note 91.

141. Global Internet Freedom Act, H.R. 4741, 109th Cong. (2006).

142. *Id.* § 4(e).

143. *See id.* § 4 ("Development And Deployment Of Technologies To Defeat Internet Jamming And Censorship").

144. *Id.* § 4(e).

145. *Id.* § 3(6).

146. *See* Global Online Freedom Act, H.R. 275, 110th Cong. § 104 (2007) (stating that the funds "are authorized to be appropriated to the Office to carry out this section," which includes duties such as "develop and ensure the implementation of a global strategy and programs to combat state-sponsored and state-directed Internet jamming").

147. H.R. 4741 § 4 ("Development and Deployment of Technologies to Defeat Internet Jamming and Censorship").

combat" Internet jamming.[148] While the office established by GOFA would not be given the explicit duty to fund anti-jamming technology in the way that GIFA would require, the office would be well within its power to do so.

GIFT signals that the issue of Internet freedom deserves more attention from non-censoring governments, including the U.S. government.[149] It includes the goal that the U.S. government work with international organizations to achieve change.[150] This commitment not to act unilaterally can be seen throughout the GIFT strategy.[151] The cooperative language of GIFT stands in contrast to the language in GIFA, which reads as a more aggressive and unilateral effort.[152] Due to GIFA's unilateral nature and the explicit funding of technology that circumvents foreign government's censorship efforts, it is important to determine what its drafters believe would be achieved through GIFA that would not be achieved through the more passive, international approach of the already existing GIFT.

C. *GIFA's Likelihood of "Promoting Democracy and Freedom"*

GIFA explicitly identifies one of its purposes as the promotion of technology that "can be used to promote democracy and freedom in countries around the world."[153] However, promotion of democracy may be wishful thinking on the part of GIFA's drafters. In China, a main target of the proposed legislation, the majority of Internet users have typically been well-educated, wealthy men in the stronger economic regions of the country.[154] Historically, the groups with Internet access have also tended to be proponents of Chinese

---

148. H.R. 275 § 104.

149. FACT SHEET, *supra* note 91.

150. *Id.*

151. *Id.* Some example excerpts of such language include: "Sustained persuasion in meetings with foreign officials: We are committed to pressing the message on Internet freedom in official dialogues with other countries." *Id.* "Coordinating with international partners: We will work with like-minded governments to promote Internet freedom and to press other governments to live up to their existing international commitments regarding freedom of expression and the free flow of information and ideas." *Id.* "Maintaining and expanding Internet freedom commitments in multilateral organizations: We will work to ensure existing international commitments to the free flow of information and freedom of expression are upheld and replicated in appropriate international fora." *Id.* "We stand ready to engage appropriately with the technology industry, non-governmental organizations (NGOs), and other stakeholders in a process aimed at developing shared principles to guide private sector activities in restrictive economies." *Id.*

152. *See generally* H.R. 4741; FACT SHEET, *supra* note 92. The more aggressive nature of GIFA can be seen in, though is not limited to, its willingness to fund software that circumvents foreign governments' firewalls without any international cooperation.

153. H.R. 4741 § 3.

154. Deans, *supra* note 19, at 135.

nationalism, rather than a liberal, reformist view.[155] Chinese nationalists have frequently published anti-American and anti-Japanese content on the Internet.[156]

According to a July 2007 report by the China Internet Network Information Center, the Internet in China "is still the tool of [those] holding higher academic degrees and has yet to be a stage for [the] common public to understand the world."[157] China had 162 million Internet users in June 2007 (second only to the U.S. with 211 million),[158] but the Internet penetration rate was only 12.3% (compared to above 65% in the U.S., Japan, and Korea).[159] That same report did, however, show trends of increasing use among less-educated users.[160] It also states, against the historical numbers, that Internet users in 2006-2007 "have a relatively low income," though this is largely influenced by the high percentage of student users.[161]

While GIFA therefore may not effectively promote democracy, as its drafters intended, circumventing the firewall would at least make information related to democracy more available within China.[162] While it is generally difficult to know exactly what the Chinese government censors or filters online, a 2002 study by Harvard Law School's Berkman Center for Internet & Society found that the top ten Google results using the keyword "equality" were all blocked, as were eight of the top ten results for keywords "democracy China" and "dissident China."[163] While studies like this likely fuel the belief of the Act's drafters that breaking down the firewall will help to promote democracy, availability of political speech does not necessarily lead to spread of such ideas. For reasons such as those discussed above, this may be especially true in China.[164]

---

155. *Id.*

156. *Id.* at 137.

157. CHINA INTERNET NETWORK INFO. CTR., STATISTICAL SURVEY REPORT ON THE INTERNET DEVELOPMENT IN CHINA 18 (2007), *available at* http://www.cnnic.net.cn/download/2007/20thCNNICreport-en.pdf.

158. *Id.* at 9.

159. *Id.* at 9-10.

160. *Id.* at 18.

161. *Id.* at 22.

162. *See China's Internet Censorship*, CBS NEWS, Dec. 3, 2002, http://www.cbsnews.com/stories/2002/12/03/tech/main531567.shtml (stating that Internet sites promoting democracy were among the most often blocked by the Chinese government).

163. *Id.*

164. *See* Deans, *supra* note 19, at 135 ["[I]n practice the groups in China that have access to the Internet have not tended to express a strong reformist view but have instead tended to promote a strong Chinese nationalism.").

D. *The U.S. Government's Domestic Curtailments of Internet Freedom*

One major concern with U.S. funding of software designed to defeat foreign governments' Internet censorship is the U.S. government's own domestic Internet policies. The Justice Department served subpoenas on Google, Yahoo!, AOL, and Microsoft's MSN in 2006 seeking "a random sampling of millions of Internet addresses cataloged in their databases, as well as for records for potentially billions of searches made over a one-week period."[165] The Justice Department wanted the information to bolster "its argument that Web-filtering software doesn't work."[166] This would in turn support the government's case for upholding the Child Online Protection Act (COPA) of 1998.[167]

COPA requires online distributors of "material harmful to minors" to keep minors from viewing such content.[168] In a 2002 case, *Ashcroft v. American Civil Liberties Union*,[169] the Supreme Court upheld an injunction barring prosecutors from filing criminal cases under COPA until after a full trial reviewing the "current technological reality" of the state of pornography-filtering applications.[170] The Court suggested that such a trial might prove that filtering is more effective than a criminal statute in preventing children from viewing pornography.[171] A U.S. district court has subsequently held that COPA is facially violative of the First and Fifth Amendments.[172] However, the Supreme Court has held that the Children's Internet Protection Act (CIPA), which requires schools and libraries to install filters to block content harmful to minors, is constitutionally valid.[173]

The U.S. norms on what is and isn't appropriate to view on the Internet have been exported through the government's sponsorship of anti-jamming software.[174] Anti-jamming technology used by the U.S. International Broadcasting Bureau (IBB), which broadcasts Voice of America, prevents its users in Iran and China from viewing websites

---

165. Maria Godoy, *Google Records Subpoena Raises Privacy Fears*, NATIONAL PUBLIC RADIO, Jan. 20, 2006, *available at* http://www.npr.org/templates/story/story.php?storyId=5165854.

166. *Id.*

167. *Id.*

168. *Id.*

169. Ashcroft v. ACLU, 535 U.S. 564 (2002).

170. Declan McCullagh, *Supreme Court Keeps Net Porn Law on Ice*, ZDNET NEWS, June 29, 2004, http://news.zdnet.com/2100-3513_22-5251475.html.

171. *Id.*

172. ACLU v. Gonzales, 478 F. Supp. 2d 775, 821 (E.D. Pa. 2007).

173. United States v. Am. Library Ass'n, 539 U.S. 194, 214 (2003).

174. *See* Declan McCullagh, *Perspective: U.S. Blunders with Keyword Blacklist*, CNET NEWS, May 3, 2004, http://news.com.com/2010-1028_3-5204405.html (discussing the U.S. government's apparent attempt to censor content accessed by individuals using its anti-jamming technology).

that include certain listed keywords.[175] This was discovered through an independent report released in 2004.[176] For China, which bases part of its firewall on blocking certain listed keywords, this amounts to U.S. sponsorship of software that essentially replaces China's censored keyword list with the United States' own list.

U.S.-imposed censorship is not confined to blatantly offensive content; the list in the IBB software includes "ass" (which inadvertently bans usembassy.state.gov), "breast" (which blocks breastcancer.com), "hot" (which blocks hotmail.com and hotels.com) and "teen" (which blocks teens.drugabuse.gov).[177] Jonathan Zittrain, a Harvard University law professor and co-author of the report, commented that "[t]he minute you try to temper assistance with evading censorship with judgments about how that power should be used by citizens, you start down a path from which there's no clear endpoint."[178]

IBB's anti-jamming software operates through Anonymizer, discussed previously.[179] The filtering list was implemented through Anonymizer at the government's behest.[180] The IBB argued that such filtering is necessary because it is inappropriate for U.S. funding to help citizens of Iran and China view pornography.[181] However, the list goes beyond blocking only pornography. A 2004 editorial article commented that the IBB list "displays a conservative bias that labels any Web address with 'gay' in them as verboten."[182] Ken Berman, who oversees the China and Iran Internet projects at IBB, called the filtering "a trade-off we feel is a proper balance."[183]

The independent report was also critical of the IBB for not choosing to use SSL encryption to scramble the browsing behavior of Iranian citizens.[184] However, the IBB responded that Iran doesn't currently monitor the content of downloaded web pages.[185] The IBB does enable SSL encryption for Chinese citizens because the Chinese government is known to monitor download content.[186]

The U.S. government's own restrictions on Internet use are not limited to pornography and sexual crime, but are also evident in the anti-terrorism arena. GOFA condemns foreign governments' monitoring of citizens' Internet activities, yet the PATRIOT Act of

---

175. *Id.*
176. *Id.*
177. *Id.*
178. *Id.*
179. *Id.*
180. *Id.*
181. *Id.*
182. *Id.*
183. *Id.*
184. *Id.*
185. *Id.*
186. *Id.*

2001 allows similar liberty curtailments in the United States. The Electronic Frontier Foundation (EFF) has listed three concerns with the PATRIOT Act: (1) expanded surveillance with reduced checks and balances; (2) overbreadth with a lack of focus on terrorism; and (3) allowing Americans to be more easily spied upon by U.S. foreign intelligence agencies.[187]

Regarding U.S. citizens' use of the Internet, EFF reads the PATRIOT Act as allowing the government to "monitor the online activities of innocent Americans, and perhaps even track what Web sites you read, by merely telling a judge anywhere in the U.S. that the spying could lead to information that is 'relevant' to an ongoing criminal investigation."[188] The person being "spied on does not have to be the target of the investigation."[189] The application must be granted, and the government is not required to report to the court or the person spied upon what is done in the investigation.[190] EFF is also concerned that the PATRIOT Act allows "nationwide roving wiretaps" which effectively mean that the "FBI and CIA can now go from phone to phone, computer to computer without demonstrating that each is being used by a suspect or target of an order, or even specifically identifying the person targeted."[191]

The PATRIOT Act also resulted in changes regarding the government's access to user information from ISPs.[192] It expands the amount of information that ISPs may voluntarily give the government absent a court order or subpoena.[193] It also expands the information which the government may obtain with a simple subpoena—which doesn't require court review—to "include records of session times and durations, temporarily assigned network (I.P.) addresses, and means and source of payments, including credit card or bank account numbers."[194] All of these changes are further strengthened by the PATRIOT Act's expanded definitions of "terrorism."[195] EFF believes that the PATRIOT Act § 802's definition of "domestic terrorism" could include legitimate domestic protest activity.[196]

---

187. ELECTRONIC FRONTIER FOUND., *EFF Analysis of the Provisions of the USA PATRIOT Act*, Oct. 27, 2003, http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php.

188. *Id.*

189. *Id.*

190. *Id.*

191. *Id.*

192. *Id.*

193. *Id.*

194. *Id.*

195. *Id.*

196. *Id.*

Incidents like the arrests in China related to political Internet activity,[197] and the coinciding fear of Chinese citizens regarding their privacy from the government on the Internet, make a strong case for international action to curb governmental Internet monitoring. However, the brief discussion above regarding the U.S.'s own Internet censorship and increasing limits on privacy shows that the unilateral action proposed by GIFA essentially replaces other countries' limits and values with those of the U.S. government. GIFA is written in language connoting an Internet free of government censorship, but in fact it proposes an Internet where the only government censoring is the U.S. government; it replaces the Chinese firewall with its own.

E. *U.S. Obscenity Law and the Community Standards Test*

The hypocrisy of U.S. government funding of anti-jamming technology is especially visible when viewed in relation to the United States' domestic obscenity law. The "community standards" test is generally used by U.S. courts to determine whether content is obscene.[198] Some, including Justice Kennedy and Justice Stevens, have questioned the community standards test's applicability to the Internet, because the test was originally intended to look at a specific local community's standards.[199] However, the plurality opinion in *Ashcroft v. ACLU* states that "[i]f a publisher chooses to send its material into a particular community, this Court's jurisprudence teaches that it is the publisher's responsibility to abide by that community's standards."[200] The opinion goes on to state that "the publisher's burden does not change simply because it decides to distribute its material to every community in the Nation."[201]

If anti-jamming software were to be funded through GIFA or GOFA, the U.S. government would continue to allow the most restrictive standard within the U.S., the community standards test, to govern; however, it would actively circumvent any more restrictive standards applied internationally. Other countries could easily view such a stance as a U.S. statement that it should be the sole judge of what is acceptable Internet content globally. This stance may be especially insulting to foreign governments if the U.S. funds subversive technological measures to effectively impose U.S. norms.

---

197. *See* Newbold, *supra* note 25, at 508.

198. *See generally* Ashcroft v. ACLU, 535 U.S. 564 (2002) (applying the "community standards" test).

199. *Id.* at 583.

200. *Id.*

201. *Id.*

IV. THE SOLUTION: FACILITATING PRIVATE ACTION

The analysis above shows that while the U.S. government must have some role in defeating Internet censorship, direct funding of anti-jamming software, as explicitly called for by GIFA and likely to occur under GOFA, is not the answer. The U.S. government should facilitate private action to defeat Internet-jamming through (1) allowing anonymization sites that are aimed at circumventing foreign government censorship to operate with minimal U.S. government involvement, and (2) attempting to minimize U.S. corporate assistance in foreign governments' censorship of the Internet.

Before discussing these two actions in more detail, it is worth summarizing why GIFA is not a good solution to the problem of Internet censorship. The establishment of GIFT accomplished much of the good that could come through GIFA. GIFT acknowledges that non-censoring countries, including the U.S., need to take active steps to break down Internet censorship, and it seeks a diplomatic, multilateral approach.[202]

As discussed above, the main addition of GIFA is the direct U.S.-government funding of anti-jamming software.[203] This additional funding coming from the U.S. government would likely have strings attached, and could both alter the nature of the anti-jamming services and reflect poorly on the U.S. government.[204] As the anti-jamming efforts can draw upon the general public through peer-to-peer technology, less funding is needed. In addition, GIFA and GOFA are worded broadly in regards to the use of the proposed funds, and could amount to a blank check to be used in efforts that only peripherally touch upon Internet censorship.[205]

The likely strings attached to the funding of existing anti-jamming software under GIFA or GOFA would be in the form of modifications—likely filtering, if not others—imposed on the services by the government. This can only be assumed because it is not explicitly written in the bills, but previous anti-jamming efforts that have involved U.S. government funding have had filtering imposed, as discussed above.[206] The U.S. government has expressed its fear of opening up the Internet in China and other censoring countries to allow pornography,[207] and this is not likely to change. What could change would be the sophistication of the filtering techniques used so as not to block as much legitimate, non-obscene content. However, such modifications and development of better filtering software would

---

202. *See supra* Part III.B.
203. *See supra* Part III.B.
204. *See supra* Part III.B, III.D.
205. *See supra* Part III.B.
206. *See supra* Part III.D.
207. *See supra* Part III.D.

be an example of funds going towards a goal that only peripherally touches upon bringing down the censoring firewall. This money would go towards allowing the U.S. government to censor on its own terms, as opposed to removing censorship completely.

It is also worth noting here that although early private efforts at anti-jamming software failed due to lack of funding, the current private efforts have become more organized and powerful.[208] This organization and strengthening can be seen in the December 2006 agreement between four of the largest companies involved in anti-jamming software.[209] These companies have expressed their confidence in locating the necessary funding to keep their services operational until China's firewall comes down.[210] At the same time, the funding required to operate anti-jamming services is drastically lowered as the services increasingly rely on public users' ability to serve as nodes or hosts in peer-to-peer systems, thus shifting bandwidth costs away from a central server.

This Note will now discuss the two prongs of the suggested approach: (1) allowing anonymization websites to operate with minimal U.S government involvement; and (2) attempting to minimize U.S. corporate assistance of foreign governments' censorship efforts.

A. *Minimizing Government Involvement in Anti-Jamming Efforts*

When the U.S. government has had a part in anti-jamming technology in the past, it has tried to limit the software's use to users of specific countries such as Iran or China.[211] The government could have many reasons for this, including worries about citizens in non-censoring countries using the software for free as a way to shield their online activity and thus wasting bandwidth, as opposed to using the site for its intended function. Another reason the U.S. government likely does not want such privacy services used by its own citizens or by users in other specific countries is the resulting increased difficulty in tracking terrorist activity.

The U.S. government needs to maintain a clear position on the operation and use of anonymization sites in order to allow private companies to know the level of services they may offer to foreign users. The approach could fall short of allowing anonymization sites to operate completely without regulation, and could include some sort of government-imposed record-keeping in order to deal with worries such as terrorism and child pornography. However, if such records were accessible by the government under the lax requirements of the

---

208. *See Milestone Agreement*, *supra* note 68 (discussing private efforts).
209. *Id.*
210. *See id.* (discussing sources of funding).
211. *See supra* Part III.D.

PATRIOT Act, the U.S. government would essentially give itself access to the very type of personal information that would be denied to other governments under GOFA.

If anonymization sites have explicit approval from the U.S. government and are allowed to operate globally without significant U.S. government-imposed restrictions, then the sites can likely gain additional private funding. If such sites could be considered by U.S. corporations as major gateways to the global Internet for users in censoring countries like China, such anti-jamming sites could likely seek funding through both imbedded advertisements and from large websites such as Yahoo! and Google that are accessed through the service. The latter would likely only come through a conjunction of this proposed prong—explicit U.S. approval of anti-jamming sites—and the second prong, which would hopefully remove the censored versions of Yahoo! and Google from China. This possibility will be discussed further below.

B. *Minimizing U.S. Corporate Assistance in Foreign Governments' Censorship Efforts*

An article written by Jill Newbold discusses various ways in which the U.S. government could impose liability on U.S. corporations for selling censorship tools to China.[212] She discusses possibilities such as liability for human rights violations under the Alien Tort Claims Act.[213] While these options may be worth exploring for blatant assistance of foreign censorship, such as providing technology that has no use other than for censorship, they should not be used against companies that merely provide a government with general-purpose Internet technology that has the ability to filter. If companies involved in the latter type of sales appear to be knowingly assisting foreign censorship, it is increasingly likely that U.S. investors will take notice as the publicity of Internet-censorship issues continues to increase.[214] GOFA's proposed feasibility study on the establishment of export license requirements for technology that facilitates restrictions on Internet freedom is a good first step to raise awareness of this issue.

Perhaps more important than preventing U.S. corporations from supplying China with censorship technology is preventing large U.S.-

---

212. Newbold, *supra* note 25.

213. *Id.*

214. *See Smith Reintroduces the Global Online Freedom Act*, OFFICE OF U.S. REP. CHRIS SMITH, Jan. 8, 2007, *available at* http://www.house.gov/list/press/nj04_smith/gofareintro.html ("Investors are taking notice of the repressive business practices of these Internet companies and are starting to voice their opposition in masses. Corporations need to heed these concerns and understand that it is good business to promote human rights, not suppress them.").

based websites like Google and Yahoo! from offering censored versions of their sites to Chinese users. The availability of these censored sites lessens the demand within China for an uncensored Internet by offering Chinese citizens something that may be "close enough" to the global Internet, making it less likely that the firewall will be broken from inside China.

Google and Yahoo! have expressed their desire for the U.S. government to give them an excuse to not censor their sites for China.[215] It is therefore probably not necessary for the U.S. government to actually prosecute U.S. corporations that merely comply with China's censorship requests. But the U.S. should put in place legislation that companies like Google and Yahoo! can use as a cover to force the Chinese government to a decision between global search engine access and Internet censorship. GOFA does not seem to be tailored to this purpose, but rather seems focused on preventing companies from giving personal information to censoring governments and creating transparency as to what content is censored. While GOFA would create some cumbersome formalities for companies such as Google and Yahoo! doing business in China, the information obtained by the U.S. government regarding censorship would help to raise public awareness of these companies' decisions, which could further discourage offerings such as the self-censored Google.cn.

If private anti-jamming efforts continue to grow and become more sophisticated, and the censored versions of sites like Google and Yahoo! are no longer offered, the Chinese firewall might be broken from inside China through the demand of Chinese citizens and government frustration in filtering efforts. If large anti-jamming options were to emerge for Chinese users with no other access to some major sites like the uncensored Google, sites like Google could probably help to fund the anti-jamming technology by sharing advertising dollars derived from Chinese viewers that would not have been realized but for the Chinese citizens' use of anti-jamming software. If the U.S. government is willing to take the suggested approach and allow private corporations to operate anti-jamming software free of government intervention, while also minimizing other U.S. corporations' assistance of China on the other side, the U.S. government funding of anti-jamming software proposed by GIFA and GOFA would not be necessary.

---

215. *See supra* Part II.E.

V. CONCLUSION

U.S. government funding of anti-jamming software is not a good approach to defeating foreign governments' Internet censorship. The U.S. government would be perceived internationally as imposing its own standards of decency and morals onto China and other countries with similar state-imposed Internet censorship. The U.S. government should facilitate private action to defeat Internet-jamming by: (1) allowing anonymization websites that are aimed at circumventing government censorship to operate with minimal U.S. government involvement; and (2) attempting to minimize U.S. corporate assistance in foreign governments' censorship efforts. If the U.S. allows anti-jamming software to operate free of government intervention while also minimizing U.S. corporate assistance of China, including pressuring the removal of self-censored versions of popular sites like Google, there is a good chance that firewalls will be broken from inside censoring countries through popular demand and government frustration.

Andrew W. Lloyd[*]

* J.D. Candidate, Vanderbilt University Law School, May 2008.