AIDING THE ENEMY: IMPOSING LIABILITY ON U.S. CORPORATIONS FOR SELLING CHINA INTERNET TOOLS TO RESTRICT HUMAN RIGHTS

Jill R. Newbold*

China's restriction on Internet access and usage by its citizens, while consistent with its Communist ideology, is contrary to international principles of the freedoms of speech and access to information as human rights that should be guaranteed to all the world's citizens. Even more appalling than China's restrictions is the fact that China's success in regulating Internet usage would not be possible without the assistance of American corporations. This Note explores the responsibilities and liabilities of American corporations to Chinese citizens and proposes a course of action that seeks to curb American involvement in denying those citizens one of the basic human rights that American citizens cherish.

I. Introduction

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist....[Y]ou are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace.... We will spread ourselves across the Planet so that no one can arrest our thoughts.

"Save us! Save us! Good people, help us! We don't want to die!" Jin Hongjiu woke in the middle of the night to screams coming from "strange, desperate" voices and thought that a fight had broken out in the streets of Beijing, China. What he saw, however, was more horrific—flames shooting from the barred windows of an Internet café and a crowd of young men trapped inside, shoving against the iron bars, screaming and waving their arms for help. Was this a terrorist act or a hostage situation? No, these young men were trapped by fear—a fear caused by

^{*} J.D., University of Illinois College of Law 2004.

^{1.} John Perry Barlow, *A Declaration of the Independence of Cyberspace*, *at* http://www.eff.org/~barlow/Declaration-Final.html (Feb. 8, 1996) (emphasis added).

^{2.} Phillip P. Pan, Fire Victims Were Locked in Café; 24 Die at Illegal Internet Shop in Beijing; Owner Bolted Door to Keep Out Police, WASH. POST, June 17, 2002, at A11.

^{3.} *Id*.

Communist China's latest efforts to implement Internet regulations. To control Internet information flow in China, the government has imposed strict regulations on cybercafés, shutting down tens of thousands during the past few years. Consequently, many cafés operate without proper licensing. This particular Internet café owner feared the "net police," and regular customers stated that the owner bolted the door at night to keep out officers and government inspectors. After twenty-four people died and thirteen others suffered injuries, Liu Qi, the mayor of Beijing, ordered the closing of all cybercafés in the city. This was done in order to give the government time to draft new regulations, calling the fire the "worst in the Chinese capital since the Communist revolution in 1949."

Although the open communication of the Internet clashes with Communist precepts of restricted speech and information access, China has embraced the Internet in an effort to spur economic development. The Communist Party remains dedicated to regulating what its citizens see and read; but it also wants private investors to drive economic growth, which requires unrestricted access by investors to information and to modern communications.⁷

Despite the Chinese government's wishes, China's growing presence in cyberspace will inevitably increase its citizens' exposure to Western democratic ideologies, especially the freedoms of speech and information access. The "desire of governments to control a medium with unprecedented possibilities for freedom of speech runs counter to the censorship-evading ethics and technology of cyberspace." China seeks to curtail exposure to liberal democratic human rights with efforts to isolate its citizens from outside influences. Initially, the Internet community assumed that "no authoritarian regime was safe from the liberating power of the Net." At this moment, the battle between new hopes and even newer technologies still rages in China. As the government's ability to constrict information flow grows, so does its citizens' demands for Internet freedom.

Despite predictions, the Chinese government largely has been successful in enforcing its Internet regulations. Web sites and Web pages

^{4.} *Id.* As of the date of the fire, the New China News Agency reported that only 200 of Beijing's estimated 2,400 cybercafés operated with the necessary permits, and other media sources estimated that between thirty to fifty percent of all cybercafés in China are unlicensed. *Id.*

^{5.} *Id*.

Id.

^{7.} Peter S. Goodman & Mike Musgrove, China Blocks Web Search Engines; Country Fears Doors to Commerce Also Open Weak Spots, WASH. POST, Sept. 12, 2002, at E1.

^{8.} TIM JORDAN, CYBERPOWER: THE CULTURE AND POLITICS OF CYBERSPACE AND THE INTERNET 144 (1999).

^{9.} JOHN F. COOPER & TA-LING LEE, COPING WITH A BAD GLOBAL IMAGE 100 (1997).

^{10.} David Lee, *Multinationals Making a Mint from China's Great Firewall*, S. CHINA MORNING POST, Oct. 2, 2002, at 16, 2002 WL 26305950.

^{11.} Sophie Beach & Xiao Qiang, As Controls Increase, "Internet Citizens" Demand More Freedom, S. CHINA MORNING POST, Oct. 3, 2002, 2002 WL 26306076 [hereinafter Beach & Qiang, Controls Increase].

are blocked; emails cannot be accessed; Internet Service Providers ("ISPs") are signing self-censorship pledges; cybercafés monitor usage and report their patrons' activities; and several people have been arrested because of their online activities. ¹² American citizens, sheltered under a blanket of democracy, should be shocked at these rigorously enforced restrictions. Even more appalling is the participation of American capitalists in China's Internet regulation. China's success "could not have happened without the help of Western firms."

China's Internet regulations block much more than "politically offensive" information. The Chinese government's reaction to the recent SARS outbreak illustrates its commitment to oppress the basic freedoms of speech and press, no matter the cost to its citizens' health and welfare. According to Senator Jon Kyl, China's efforts to withhold and block information about the SARS outbreak placed thousands of lives at risk. SARS serves as a chilling omen of the impact the Chinese government's stranglehold on information flow has on both the Chinese people and the world community.

The following discussion focuses on the role that United States corporations play in furthering China's ability to regulate the Internet. Part II examines China's Internet restrictions, while Part III discusses American corporate involvement in marketing the technological improvements necessary to enforce these restrictions. Part III also discusses the applicable international human rights issues and potential sources of United States corporate liability for assisting China in suppressing the freedoms of speech and access to information. Part IV proposes that the United States provide a federal forum for Chinese citizens who seek redress against corporations and calls upon Congress to seek an international resolution condemning China's human rights violations.

II. BACKGROUND

This section will first discuss the underlying Communist ideologies throughout China which serve as motivation for its Internet regulations. Next, this section highlights the legal regulations operating to modify the behavior of both individual Internet users in China and ISPs seeking to operate in the state. Finally, this section will explore the technological

^{12.} Lee, supra note 10.

^{13.} *Id*.

^{14.} Press Release, Federal Document Clearing House, SARS Outbreak Shows Freedoms Still Chilled in China, Kyl Tells Commission Senator Urges Support for Legislation to Aid Chinese Citizens' Information Access (June 5, 2003), 2003 WL 11710092.

^{15.} *Id*

^{16.} Sars in China: Implications for Information Control, Internet Censorship, and the Economy: Hearings Before the U.S.-China Economic and Security Review Comm., 108th Cong. *12 (2003) (statement of Sen. Jon Kyl), available at http://www.uscc.gov/hearings/2001_02hearings/transcripts/02_06_05tran.pdf (June 5, 2003) [hereinafter SARS in China].

barriers to Internet access as methods of enforcing these legal promulgations.

A. A Democratic Economy and Communist Government Clash

In line with its Confucian¹⁷ beliefs, the Chinese Communist Party ("CCP") launched an oppressive political campaign in 1966, known as the Cultural Revolution, ¹⁸ to foster "impersonal, ideologically correct, and universal relationships" in China, but this effort failed. ¹⁹ Lasting until 1976, ²⁰ the ten years of the Cultural Revolution isolated China from the outside world, causing it to fall far behind other developed nations. ²¹ Although China continued to see itself as a world power due to its size, traditions, and population, isolation from the technical world over the last two centuries was a factor hindering its status as an actual world power. ²² Because modernization was one of the few overarching ideologies left in China, it had little choice but to introduce the Internet into its communications structure. ²³

When China opened the door to more developed technology, it also opened the door to political upheaval and the dangers accompanying technological change. In 1989, Zhao Ziyang, a member of China's Thirteenth Congress stated:

I have more and more deeply realized that reform of the political structure can neither surpass nor lag behind economic structural reform.... In the past, I thought that as long as economic structural reform was successful and the economy developed, then the people's living standards would be enhanced and the people would be satisfied as society would be stable. I later found that this was not the case in reality. With the enhancement of people's living standards and cultural attainments, they will have a stronger sense

^{17.} Clara Liang, Red Light, Green Light: Has China Achieved Its Goals Through the 2000 Internet Regulations?, 34 VAND. J. TRANSNAT'L L. 1417, 1425 (2001). The Confucian principle is known as the Rule of Man, under which each person finds his or her role in society by using relationships as guidance, and unity prevails over individualism. Id. at 1426.

^{18.} Timothy L. Fort & Liu Junhai, Chinese Business and the Internet: The Infrastructure for Trust, 35 VAND. J. TRANSNAT'L L. 1545, 1580 (2002).

^{19.} XIAOBO LÜ, CADRES AND CORRUPTION: THE ORGANIZATIONAL INVOLUTION OF THE CHINESE COMMUNIST PARTY 134–35 (2000). It is agreed that Mao Zedong launched the Cultural Revolution out of his discontent with the growing bureaucratization of the CCP and its officials. *Id.* One major goal of the Revolution was to "weed out the values of exploitative classes, replacing them with Communist values or what may be called *public*-ism." *Id.* at 135–36. Instead of creating a new class of *public* human relations, the Revolution created a basis for some long-standing informal relationships, weakening many of China's already fragile institutions and organizational norms. *See id.* at 135–37.

^{20.} Fort & Junhai, supra note 18, at 1580.

^{21.} Richard Cullen & Pinky D. W. Choy, *The Internet in China*, 13 COLUM. J. ASIAN L. 99, 107 (1999).

^{22.} Id. at 108.

^{23.} See id.

of political participation and will long for democracy more strongly.²⁴

China has already experienced the disastrous effects of advanced communications. China's regulation of the Internet can be traced back to the events at Tiananmen Square and the government's desire to avoid reliving another human rights tragedy of similar magnitude.²⁵ Tiananmen, the military killed 7,000 protestors and over 20,000 protesters were wounded.²⁶ During the Student Democratic movement in 1989, political protestors used facsimile machines—cutting-edge technology at the time-to exchange information and release it to the outside world.²⁷ The Tiananmen movement alerted the Chinese government to the Internet's abilities, as it saw students making use of the limited Internet connections available at local universities.²⁸ The Chinese government has not forgotten Tiananmen and the role of communications technology in the quashed democratic movement. It views the Internet, a tool far more powerful than facsimile machines, with a correspondingly greater suspicion.²⁵

B. Legal Regulations

The State Council is the executive branch of the National People's Congress and the highest authority of state administration with the power to enact nationwide law.³⁰ The State Council created the Internet regulations and depends on numerous ministries for enforcement, each ministry having its own specific jurisdiction.³¹

On February 1, 1996, the State Council enacted the "Interim Provisions Governing Management of Computer Information Networks

- 24. MICHAEL E. MARTI, CHINA AND THE LEGACY OF DENG XIAOPING 25–26 (2002).
- 25. Liang, supra note 17, at 1427.
- 26. James Conachy, Ten Years Since the Tiananmen Square Massacre: Political Lessons for the Working Class, at http://www.wsws.org/articles/1999/jun1999/tian-j04.shtml (June 4, 1999).
 - 27. Cullen & Choy, supra note 21, at 109–10; Liang, supra note 17, at 1427.
- 28. Scott E. Feir, Regulations Restricting Internet Access: Attempted Repair of China's Great Wall Restraining the Free Exchange of Ideas, 6 PAC. RIM L. & POL'Y J. 361, 367 (1997).
 - 29. Cullen & Choy, supra note 21, at 110.
 - 30. Feir, *supra* note 28, at 368–69; Liang, *supra* note 17, at 1431.
- 31. Liang, *supra* note 17, at 1431. In 1998 the Ministry of Information Industry ("MII") was established to oversee telecommunications, satellites, and the Internet, and it is primarily responsible for regulating all Internet activities in China, including ISPs. Jiang-yu Wang, *The Internet and E-Commerce in China: Regulations, Judicial Views, and Government Policies,* 18 COMPUTER & INTERNET L. 12, 13 (2001). The Ministry of Public Security ("MPS") oversees Internet security regarding mandatory registration by Internet users and prevents dissemination of prohibited content. *See id.* at 14. As part of enforcing the Internet regulations, Internet users were ordered to register with the MPS within thirty days of receiving a warning notice from the government. Feir, *supra* note 28, at 370. Those who fail to comply are "severely dealt with" by the MPS. *Id.*

The MPS has the power to investigate computer crimes, furnish computer security training, and implement computer security regulations. Liang, *supra* note 17, at 1432. The "police of Chinese society" protect the Internet from being used to "leak state secrets, conduct political subversion, or spread pornography or violence." Cullen & Choy, *supra* note 21, at 114. The People's Liberation Army, whose main purpose is general security in China, also takes part in the security and enforcement of Internet regulations. *Id.* at 115.

in the People's Republic of China Connecting to the International Network" ("Provisions"),³² marking the CCP's first key effort to control the Internet via regulations carrying the force of law.³³ Article 13 of the Provisions specifically prohibits certain Internet conduct and content:

No unit or individual may use the Internet to engage in criminal activities such as harming national security or disclosing state secrets. No unit or individual may use the Internet to retrieve, replicate, create, or transmit information that threatens social stability and promotes sexually suggestive material.³⁴

Violators of the Provisions are subject to various punishments, depending on the article violated.³⁵ Dozens of Chinese citizens have been imprisoned for political activity on the Internet.³⁶ The U.S. State Department reports that one individual was "bound by hand and foot and beaten by police while they tried to force him to confess to subversion" after posting information about students who disappeared in the Tiananmen Square protests.³⁷

In 1998, China passed its second major set of Internet regulations, called the "Provisions for the Implementation of the Interim Provisions Governing the Management of Computer Information Networks in the People's Republic of China"³⁸ which mandated restricted networks and government approval of ISPs.³⁹ Both individual users and ISPs share liability for illegal content on the Internet under China's unique approach to Internet regulation.⁴⁰ In September 2000, Premier Zhu

^{32.} Cullen & Choy, supra note 21, at 119.

^{33.} Liang, *supra* note 17, at 1431. Most of the initial Provisions involved controls over international connections to the Internet, and prescribed specific, authorized uses for the Internet. *Id.* at 1431; Cullen & Choy, *supra* note 21, at 119. The Provisions apply to Computer Information Networks ("CINs") Connecting to the Worldwide Internet ("CTWI") and defined CTWIs as "CINs within [China's] borders connecting to *foreign* CINs in order to facilitate *international* information exchange." Secretary Bureau of the State Council General Office, PRC Interim Provisions on the Regulation of Computer Networks and the Internet, (Feb. 1, 1996), *at* http://www.chinaonline.com/issues/internet_policy/regulations/c9091708.asp (emphasis added) [hereinafter PRC Interim Provisions].

^{34.} PRC Interim Provisions, *supra* note 33, at art. 13.

^{35.} For instance, individuals who fail to register before accessing the Internet under Article 10 "will be warned, then publicly criticized, then forced to terminate networking activities, and may be fined a maximum of RMB 15,000 (U.S. \$1,800)." *Id.* at arts. 10, 14.

^{36.} HOUSE POLICY COMMITTEE, POLICY STATEMENT, ESTABLISHING GLOBAL INTERNET FREEDOM: TEAR DOWN THIS FIREWALL, *at* http://policy.house.gov/html/news_item.cfm?id=112 (Sept. 19, 2002) [hereinafter TEAR DOWN THIS FIREWALL].

^{37.} Id.

^{38.} Cullen & Choy, *supra* note 21, at 122. The Implementation Measures came into effect on March 6, 1998, and in one sense, reiterate the 1996 Provisions. *Id.*

^{39.} Wang, *supra* note 31, at 13. Together with the 1996 Provisions, the 1998 regulations established a four-tier system for China's international Internet access: (1) all connections to international networks must go through the only international gateway opened by the MII; (2) only ISPs approved by the State Council, called "interconnected networks," may directly connect to the Internet through the MII gateway; (3) other ISPs, called "Internet access networks," must subscribe to one of the interconnected networks to gain Internet access; and (4) individual Internet users can access the Internet, subject to liability for violating the regulatory provisions. *Id.*

^{40.} Shamoil Shipchandler, The Wild Wild Web: Non-regulation as the Answer to the Regulatory Question, 33 CORNELL INT'L L.J. 435, 452 (2000) (comparing China's regulatory schemes with those of

Rongji signed into law the "Measures for Managing Internet Information Services" ("Measures"). The Measures were the CCP's first efforts to prevent ISPs from providing prohibited information. The Measures also regulate Internet information services ("IIS"), 42 by requiring selfmonitoring and self-censorship.⁴³ IIS providers must display their licenses and record numbers on the home page of their Web sites and guarantee that their information is legal, requiring heavy censorship to avoid hefty fines.⁴⁴ Additionally, each time a subscriber accesses the Internet, the ISPs must record when the access occurred, the subscriber's account number, addresses of all Web sites visited, and the telephone number used to access the Internet. ISPs must keep these records for sixty days and supply them to the authorities upon demand. 45 Furthermore, ISPs and IISs are restricted from circulating information that might harm the state's honor, cause ethnic oppression, spread rumors, disrupt social stability, spread pornography, undermine state religious policy, or preach the beliefs of evil cults.

IISs violating any part of the Measures are subject to a suspension of their business operations or the shutting down of their Web sites. ⁴⁷ For example, the Chinese government blocked access to the search engines Google and AltaVista in early September 2002, ⁴⁸ after Chinese officials discovered that Google users could access sites maintained by advocates for Tibetan independence, in addition to Web sites operated by the Falun Gong religious group, which the government has banned as a cult. ⁴⁹ Google's blockade was eventually lifted after millions of users

Germany and the United States, and holding China's scheme to be a combination of the other two with an added twist—ISP liability and the intimidation of the individual user).

- 43. Liang, supra note 17, at 1435.
- 44. Id. at 1436.
- 45. *Id*.

- 47. Wang, *supra* note 31, at 15.
- 48. Goodman & Musgrove, *supra* note 7 (noting that typing in the URL of these search engines produced error messages as if the pages did not exist).
- 49. *Id.* According to knowledgeable sources, the government denied access to Google after learning that a search using the term "Jiang Zemin"—the name of China's president—delivered a plethora of articles from banned newspapers that discussed the conspiracy surrounding the November

^{41.} Liang, *supra* note 17, at 1435. Article 1 of the Measures states: "These measures are drawn up for the purpose of regulating Internet information services (IIS) and promoting the healthy and orderly development of such services." *Id*.

^{42.} *Id.* IIS is defined as "services that provide Internet users with information via the Internet." *Id.* at 1435 n.140. IIS is divided into commercial providers and non-commercial providers. *Id.* at 1435 n.141. Commercial providers are defined as those that provide Internet users with information in exchange for compensation or Web page creation services. *Id.* at 1435 n.142. The Measures most likely define commercial providers broadly to include not only those providers charging access to their sites, but also those providers who charge nothing but generate income from companies advertising on their sites. *Id.* The Measures require commercial providers to apply to the local IIS administration or MII for a license to operate an "IIS value-added telecommunications business." *Id.* at 1435 n.147. Non-commercial providers are defined as those providing Internet users with open source and shared-information services on a non-profit basis. Wang, *supra* note 31, at 14.

^{46.} *Id.* This list is very similar to the 1996 Provisions, and some argue that it was issued to remind citizens and officials to obey the old rules. *Id.* However, due to the unstable rule of law in China, the Measures provide more details on topics covered by the 1996 Provisions. *Id.* at 1437.

posted protest messages, but users still can only access search results that meet the government's approval.⁵⁰

One of the most recent additions to the Internet regulations resulted from the June 17, 2002, cybercafé fire in Beijing.⁵¹ Effective November 15, 2002, the new restrictions impose stricter safety standards and requirements for licensing businesses that offer Internet access to users who pay per session.⁵² As well as heavier content and use regulation, the new laws ban minors from the cafés and require operators to register users, keep records of which information users access, and provide these records to the authorities upon request for up to two months after the information was accessed.⁵³ Owners must also install "Internet Police 110" software, which filters out more than 500,000 banned sites.⁵⁴ In addition, operators must post a sign warning users not to access or download information containing prohibited content, which includes visiting politically sensitive or gambling Web sites.⁵⁵ Violators face up to 15,000 yuan (U.S. \$1,800) in fines.⁵⁶

Since the Beijing fire, China also has imposed more severe restrictions on ISPs. On August 1, 2002, the government, recognizing that censoring millions of Web sites is an overwhelming task, enacted regulations requiring ISPs to self-censor their sites or risk being shut down. Before the new regulations were enacted, more than 300 businesses, government offices, universities, and other organizations, including ISPs, signed a voluntary, government-sponsored "Public Pledge on Self-Discipline for the China Internet Industry" ("Pledge"). In compliance with the Pledge, "[s]ignatories agree to refrain from producing, posting or disseminating harmful information that may jeopardize state security and disrupt social stability. Some Western corporations have signed the Pledge, prompting much controversy.

²⁰⁰² Congress of the Communist Party. The articles were found in Chinese-language newspapers located in Taiwan, Hong Kong, Australia, and the United States. *Id.*

^{50.} Beach & Qiang, *Controls Increase*, *supra* note 11. Millions of Chinese citizens used Google because of the power and speed of its searches and its excellent Chinese-language search capacity. *Id. See* Goodman & Musgrove, *supra* note 7.

^{51.} See supra pp. 491–92 and notes 2, 4; Beijing Approves New Measures Restricting Use of Cybercafés, ASIAN WALL ST. J., Oct. 14, 2002, at A3 [hereinafter Beijing Approves New Measures].

^{52.} Beijing Approves New Measures, supra note 51, at A3; Christopher Bodeen, China Imposes New Web Café Rules, AP ONLINE, Oct. 11, 2002, 2002 WL 101561002.

^{53.} Beijing Approves New Measures, supra note 51.

^{54.} Xiao Qiang & Sophie Beach, *The Great Firewall of China*, L.A. TIMES, Aug. 25, 2002, at M3, available at 2002 WL 2498912 [hereinafter Qiang & Beach, *Firewall*].

^{55.} Beijing Approves New Measures, supra note 51, at A3.

^{56.} *Id*.

^{57.} Qiang & Beach, Firewall, supra note 54.

^{58.} *Id.*; David Murphy, *Access Denied: As More Chinese Go On-Line, the Government Is Exerting More Control Over What They See*, FAR E. ECON. REV., Sept. 26, 2002, at 42, *available at* 2002 WL 24511990. The Pledge, organized by the Internet Society of China, aims to promote Internet use, prevent online crime, foster healthy industry competition, and avoid intellectual property violations. Ted Anthony, *Yahoo! Probe Risks Complicity*, AP ONLINE, Aug. 10, 2002, 2002 WL 25137968.

^{59.} Qiang & Beach, Firewall, supra note 54.

C. Technological Barriers

In addition to legal regulations, China also physically limits information access to the Internet. In 1996, China essentially created a large Intranet by constructing a nationwide firewall. Filtering programs block prohibited information by using site addresses or keywords that are amalgamated into the firewall system. Although the use of firewall technology is extremely efficient for Internet security–especially for China whose black-and-white ideology allows it to draw a definitive line between permissible and impermissible information—the rerouting of information to avoid a firewall remains possible.

Despite potential problems with filtering software, China continues to use and upgrade its filtering techniques. In September 2002, the Chinese government began using more sophisticated software-filtering technology that blocks selected portions of Web sites and emails according to keyword searches. For example, Chinese Internet users can now visit the previously-blocked BBC Web site and access soap opera summaries, but only have restricted access to information about current events. According to Michael Robinson, Chief Technical Officer of Beijing-based Clarity Data Systems, Chinese authorities are "re-purposing corporate-security software," allowing users to access Web

^{60.} William Yurick & Zixiang Tan, The Great (Fire)Wall of China: Internet Security and Information Policy Issues in the People's Republic of China §4.2.1 (Oct. 7, 1996) (unpublished manuscript, on file with the Telecommunications Policy Research Conference), at http://www.tprc.org/abstracts/tan.txt. A firewall is a "computer or group of computer systems that enforces an access control policy between two networks by blocking traffic or permitting traffic." Id. A firewall places a computer between the global Internet and the nation's Intranet which filters our packets of prohibited information according to a set of rules. Liang, supra note 17, at 1429–30. An Intranet is a vehicle for connecting its members to information that can be controlled by authorities. Id. at 1429. China's Intranet is an isolated and regulated Internet that allows the CCP to monitor both Web use in general and patterns of individual use. Id.

^{61.} Feir, *supra* note 28, at 376–77.

^{62.} Liang, *supra* note 17, at 1430–31. For a firewall to be effective, information must pass through it; Internet traffic that can route information around the firewall is a threat to the wall's security success. *Id.* Because the Internet was developed originally by the United States Department of Defense to maintain communications between agencies in times of war, the Internet was purposefully designed to counter even the most difficult blocking techniques. John T. Delacourt, *The International Impact of Internet Regulation*, 38 HARV. INT'L L.J. 207, 217–18 (1997).

Some argue that although firewall technology is efficient in a broad sense, it will not be able to conquer language and, in trying, it will do substantial harm along with the good China is seeking. First, filtering software attempts to control information using predetermined keywords and, because it lacks accuracy, sites containing helpful information may be blocked. Feir, *supra* note 28, at 378. For example, firewalls programmed to filter out the word "sexually" will deny users access to sites containing information regarding sexually transmitted diseases. Second, filtering software is unable to filter out material from those providers who deliberately disguise objectionable information or resort to double meanings and innuendos. Delacourt, *supra* note 62, at 231. Filtering software therefore cannot compensate for the infinite number of contexts in which a key word is used, leading to overand under-screening. *Id.* at 230.

^{63.} Beach & Qiang, *Controls Increase, supra* note 11. These software filters are used at the level of ISPs and cybercafés. Thomas Crampton, *China's "Great Firewall" Limits Internet*, INT'L HERALD TRIB., Oct. 1, 2002, at 1, *available at* 2002 WL 2889007.

^{64.} Crampton, supra note 63.

sites, but blocking certain pages or emails using packet filtering.⁶⁵ Packet filtering analyzes each bit and byte entering and leaving to see if it meets specific programmed criteria.⁶⁶ These more sophisticated filtering software restrictions can cause selective blocking of emails containing certain keywords, create difficulty in accessing foreign sites that use secure connections, and continually interrupt searches on specified topics through search engines.⁶⁷ Previously, users seeking access to prohibited information would be entirely unable to reach addresses containing this information, but emails were left free from interference. Now there is more access to the Web sites, but emails can be blocked.⁶⁸

III. ANALYSIS

This section explores two possible theories by which the involvement of U.S. corporations in enforcing China's Provisions could be curbed. Chinese citizens could sue the United States corporations in United States federal courts for civil damages under the Alien Tort Claims Act. As an alternative, Congress could adopt legislation calling for federal funds to help Chinese citizens evade the Internet restrictions and adopt an international resolution condemning the Chinese government's activity.

A. United States Corporations Aid China in Denying Human Rights

The Internet is premised upon a cyberworld of universal human rights, especially the freedom of speech and the freedom of information access. ISPs are supposed to have a liberating influence, providing materials on all topics for all to see. In China, ISPs must comply with strict Communist regulations or lose access to the world's second largest Internet market—approximately 56.6 million Internet users. The Chinese government has used the appeal of its enormous market to persuade American ISPs to self-censor in exchange for approval to operate in China. The Chinese government benefits not only from the economic boost of international investments, but profits because self-

^{65.} Murphy, *supra* note 58 (noting that the latest controls rely on "souped-up" versions of corporate firewalls).

^{66.} Crampton, supra note 63.

^{67.} *Id.* According to Ben Edelman, a technology research analyst at the Berkman Center of Internet and Society at Harvard Law School, "[t]he government now appears to have started deploying a more focused and granular filtering system." *Id.*

^{68.} *Id*

^{69. 28} U.S.C. § 1350 (2000).

^{70.} China Has the World's Second-Largest Home Internet Population, CHINA ONLINE, Apr. 22, 2002, 2002 WL 10273723. China is second only to the United States according to Nielson/NetRatings in Shanghai. *Id.* Statistics show that if twenty-five percent of people in China had access to the Internet, the country would have 257 million Internet users. *Id.* In addition, statistics from the MII demonstrate that the monthly growth rate of Internet users in China is between five and six percent. *Id.*

^{71.} Goodman & Musgrove, supra note 7, at E4.

censorship by ISPs is both inexpensive and efficient.⁷² ISP liability relieves the government from the responsibility of constantly updating regulations for technological changes, instead leaving this task to the ISPs.⁷³ China's Internet market lured over 300 Pledge signatories, and those who violate the Pledge are suspended or expelled from doing business in China.⁷⁴

Not only are American ISPs "throwing Web principles out of the window" by signing the Pledge, they are also spending hundreds of millions of U.S. dollars to conform to China's censorship requirements by training personnel and by purchasing and maintaining equipment. Yahoo!, an ISP who built its brand name by advertising as a liberating force, signed the Pledge in March 2002, while AltaVista chief executive James Barnett vowed that his company is unlikely to follow suit, stating, "[t]here's a business issue here, but there's a much more important and broader issue as well. . . . Censorship just flies in the face of everything we're all about as a company. We're about open access to information."

Equally appalling, American technology companies provide China with the software to enforce its filtering scheme. Prominent American corporations, including Cisco Systems, Microsoft, Nortel Networks, Websense, and Sun Microsystems, have all played a part in quickly equipping China with censoring equipment. 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. Democracy, it seems, takes a back seat to profitable markets. While the United States uses one hand to fight the harsh policies of Communism, its other hand feeds those same policies by allowing ISPs and American technology companies to reap the benefits of assisting China's censorship campaign.

^{72.} Lawrence Lessig & Paul Resnick, Zoning Speech on the Internet: A Legal and Technical Model, 98 MICH. L. REV. 395, 413 (1999). Lessig and Resnick note that just as the government can more easily regulate telephone companies than telephone users, it would be easier for the Chinese government to impose requirements on ISPs, which ISPs could then enforce upon their users. Id.

^{73.} Shipchandler, supra note 40, at 455.

^{74.} Anthony, supra note 58.

^{75.} Murphy, *supra* note 58. Experts believe the ISPs are using scanning technology similar to corporate firewall software that is able to block access to sites and detect viruses. *Id.* However, two Harvard researchers discovered that this software was imperfect since sites manufactured by the U.S. Central Intelligence Agency, Human Rights in China (an American-based human rights group critical of the Chinese government) and Radio Free Asia (an American government-funded radio station banned in China) were all available to Chinese Net surfers. *Id.*

^{76.} Goodman & Musgrove, supra note 7, at E4.

^{77.} Lee, *supra* note 10. According to Greg Walton, a researcher for the International Centre for Human Rights and Democracy based in Montreal, China could not possibly have developed such a sophisticated censoring system so quickly without the help of Western technology suppliers. *Id.*

^{78.} Id.

B. The Freedoms of Speech and Access to Information are Express Human Rights in Both the Domestic and International Arenas

Freedom of speech and freedom of access to information are rights inherent in the democratic promise exemplified by the United States, both domestically and abroad. U.S. laws support broad access to information at all levels of government.⁷⁹ In the international context, the United Nations passed the Universal Declaration of Human Rights ("UDHR").80 Numerous countries, including the United States, have signed the United Nations International Covenant on Civil and Political Rights ("ICCPR"), which proclaims that recognition of the "inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world."81 Both documents state that an individual shall have the right to the freedom of expression, which includes the freedom to "seek, receive and impart information and ideas of all kinds . . . through any . . . media of his choice."82 The United States not only has dedicated itself to the furtherance of this principle, but more importantly, China, as a member of the United Nations, has implicitly dedicated itself to promoting the freedom of speech and the freedom of access to information as fundamental rights of its citizens.

In Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'antisemitisme, ⁸³ a U.S. district court expressed its disapproval of a French court's decision that required an American ISP, Yahoo!, to censor material on one of its Web sites in a manner similar to that imposed by the Chinese regulations. ⁸⁴ France prohibits the sale of Nazi material and found that Yahoo.com, a Yahoo! service operating under the laws of the United States, displayed Nazi artifacts for sale on its auction site accessible by French Web users. ⁸⁵ The French court took action similar to that of China, by mandating that Yahoo! take all necessary measures to restrict access to the Yahoo.com auction service and to any other site that may be construed as an apology for Nazism or Nazi crimes. ⁸⁶ In upholding

^{79.} Harlan J. Onsrud, *Legal Access to Geographic Information: Measuring Losses or Developing Responses*?, *in* Information, Place, and Cyberspace 303, 304 (D.G. Janelle & D.C. Hodge eds., 2000).

^{80.} Universal Declaration of Human Rights, pmbl., G.A. Res. 217A, U.N. GAOR, 3d Sess., U.N. Doc. A/810, at 71 (1948) [hereinafter Declaration of Human Rights].

^{81.} International Covenant on Civil and Political Rights, pmbl., G.A. Res. 2200A, U.N. GAOR., 21st Sess., Supp. No. 16, at 52, U.N. Doc. A/6316 (1966) (entered into force Mar. 23, 1976), available at http://www.hrweb.org/legal/cpr.html [hereinafter Covenant on Civil and Political Rights].

^{82.} Id. at art. 19; Declaration of Human Rights, supra note 80, at art. 19.

^{83. 169} F. Supp. 2d. 1186, 1194 (N.D. Cal. 2001).

^{84.} Id. at 1194.

^{85.} Id. at 1184.

^{86.} Id. at 1185. The French court entered an order requiring Yahoo! to:

⁽¹⁾ eliminate French citizens' access to any material on the Yahoo.com auction site that offers for sale any Nazi objects, relics, insignia, emblems and flags; (2) eliminate French citizens' access to Web pages on Yahoo.com displaying text, extracts, or quotations from *Mein Kampf* and *Protocol of the Elders of Zion*; (3) post a warning to French citizens on Yahoo.fr that any search through

Yahoo!'s right to display the material on its United States service, the court held that to decide the case in accordance with the Constitution and the laws of the United States, "it necessarily adopts certain value judgments embedded in those enactments, including the fundamental judgment expressed in the First Amendment that it is preferable to permit the non-violent expression of offensive viewpoints rather than to impose viewpoint-based government regulation upon speech."87 Thus, the French order was not enforceable by a United States court, and the court held that compliance with the French order would involve an impermissible First Amendment restriction.⁸⁸ In line with the U.S. district court's holding, American ISPs restricting United States operations in compliance with Chinese law have a free speech defense against any enforcement of Chinese penalties. The author is not expressing sympathy for those ISPs choosing to subject themselves to Chinese laws by pointing out this similarity between governmental actions of France and China. The author's motivation for using the Yahoo! case is to display the United States' strong commitment to upholding the inherent freedoms of speech and access to information. The Yahoo! court extended this commitment to cyberspace and to international relations. It is shameful and duplicitous for the United States to throw this commitment to the side by allowing American corporations to aid China in its suppression of these freedoms.

Chinese Internet users have latched onto democracy through cyberspace and protest China's mounting restrictions. Over one thousand Web publishers and more than two hundred Chinese citizens have signed the Declaration of Internet Citizens' Rights, a document initiated by prominent writers, lawyers, and private webmasters demanding free expression and freedom of information based on the United Nations declarations.⁸⁹

Yahoo.com may lead to sites containing material prohibited by Section R645-1 of the French Criminal Code, and that such viewing of the prohibited material may result in legal action against the Internet user; (4) remove from all browser directories accessible in the French Republic index headings entitled "negationists" and from all hypertext links the equation of "negationists" under the heading "Holocaust."

Id. at 1184–85. Under the terms of the order, Yahoo! was subjected to a penalty of 100,000 Euros for each day it failed to comply with the order. *Id.* at 1185.

^{87.} Id. at 1187.

^{88.} *Id.* at 1194. The court held that France could not seek enforcement in the United States of its order impeding the First Amendment rights of Yahoo.com, Yahoo!'s U.S. service. *Id.* However, the court noted that the holding does not intend to disturb the French court's application of French law or its orders with respect to Yahoo!'s actions in France, which deal with the restrictions to be implemented on Yahoo.fr, the host's regional Web site that operates under French laws. *Id.* at 1183, 1194.

^{89.} Beach & Qiang, Controls Increase, supra note 11.

C. Holding United States Corporations Liable for Human Rights Violations Is Possible Under the Alien Tort Claims Act

Congress enacted the Alien Tort Claims Act ("ATCA")⁹⁰ in 1789 as part of the Federal Judiciary Act.⁹¹ This statute gives the federal district courts "original jurisdiction of any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States."⁹² In *Filartiga v. Pena-Irala*,⁹³ the United States Court of Appeals for the Second Circuit held that the "law of nations" included established norms of international human rights⁹⁴ and recognized that the ATCA provided for the adjudication of human rights violations.⁹⁵ In theory, Chinese citizens could sue China or Chinese government officials for restricting their speech and information access in cyberspace under the ATCA.⁹⁶

Claims against China as a state are likely to fail. As a state, China is entitled to sovereign immunity. In *Argentine Republic v. Amerada Hess Shipping Corporation*, ⁹⁷ the United States Supreme Court rejected the argument that the ATCA could be an exception to the Foreign Sovereign Immunities Act ("FSIA") ⁹⁸ and held that the FSIA is "the sole basis for obtaining jurisdiction over a foreign state in our courts." Because the FSIA contains no exceptions for violations of international law, Chinese plaintiffs would have no redress in United States courts against their country due to lack of jurisdiction.

Furthermore, both China and its government officials are likely to claim the act of state doctrine as a defense: "The courts of one country will not sit in judgment on the acts of the government of another, done within its own territory." The U.S. Supreme Court, in *Banco Nacional de Cuba v. Sabbatino*, held that the act of state doctrine dictates that United States courts may not inquire into a foreign government's actions

^{90. 28} U.S.C. § 1350 (2000)

^{91.} Eric Gruzen, The United States as a Forum for Human Rights Litigation: Is This the Best Solution?, 14 Transnat'l Law. 207, 210 (2001).

^{92. 28} U.S.C. § 1350.

^{93. 630} F.2d 876 (2d Cir. 1980).

^{94.} *Id.* at 880 (holding specifically that the act of torture committed by a state actor violated "established norms of international law of human rights, and hence the law of nations").

^{95.} Gruzen, supra note 91, at 216.

^{96.} This statement assumes that freedoms of speech and access to information are included in the law of nations, as required by the text of the ATCA. The subject is discussed in further detail under Part III, section C, subsection 2, *infra*. For purposes of immediate discussion, the author requests the reader to assume these freedoms to be actionable under the ATCA.

^{97. 488} U.S. 428 (1989).

^{98. 28} U.S.C. § 1604 (1976). The rule states:

Subject to existing international agreements to which the United States is a party at the time of enactment of this Act a foreign state shall be immune from the jurisdiction of the courts of the United States and of the States except as provided in sections 1605 to 1607 of this chapter.

Id. (emphasis added).

^{99.} Amerada Hess, 488 U.S. at 434.

^{100.} Underhill v. Hernandez, 168 U.S. 250, 252 (1897).

^{101. 376} U.S. 398 (1964).

in that government's own territory, even when the government's conduct violates international law. Therefore, claims against China and its government officials based on international human rights law could possibly be dismissed under the act of state doctrine.

Although America has little chance of conquering China's Communist principles overnight, it could fight this battle on the home front. Holding American corporations liable for their assistance to China—or banning the involvement of American corporations altogether—will force China to seek new assistance in maintaining its filtering software. Doing so will send the message that the United States will play no part in the denial of freedoms that should be guaranteed to all persons.

1. Corporations Can Be Liable Under the ATCA

The imposition of human rights duties on corporations has become an emerging trend in international law, because of economic globalization. After World War II, the second Nuremberg trials sparked legal awareness of corporate responsibility for human rights, as American courts sitting in occupied Germany declared that reprehensible acts of corporations could not "be differentiated from acts of plunder or pillage committed by officers, soldiers, or public officials of the German Reich." Nuremburg's landmark decisions, coupled with international consensus as to corporate responsibility, established the foundation for holding corporations responsible for respecting human rights.

The Second Circuit's ruling in *Kadic v. Karad ic*¹⁰⁴ expressly affirmed that private actors could be held liable for violations of the law of nations; private actors are therefore susceptible to jurisdiction under the ATCA. The Ninth Circuit in *John Doe v. Unocal Corporation* allowed foreign plaintiffs to sue a California-based corporation for forced labor even though the corporation had little connection to the

^{102.} Id. at 401.

^{103.} Steven R. Ratner, Corporations and Human Rights: A Theory of Legal Responsibility, 111 YALE L.J. 443, 477–78 (2001). The trend of corporate human rights liability continued with standards in international labor law, international environmental law, and anti-corruption law. Id. at 478–82. Furthermore, the United Nations has imposed economic sanctions for human rights violations, and although directed at states, the General Assembly and Security Council have noted that sanctions also create a duty upon corporations. Id. at 483. Practices in the European Union also illustrate this trend, as the binding decisions of the European Council and Commission have created numerous legal obligations that apply to corporate entities. Id. at 484. Finally, treaties have been interpreted to bind corporate entities as well as states, and various states have made statements about the behavior of corporate entities. Id. at 485–86.

^{104. 70} F.3d 232 (2d Cir. 1996).

^{105.} *Id.* at 239. The court considered early examples of the application of the law of nations to private acts, such as the prohibition against piracy, slave trade, and certain war crimes. *Id.*

^{106. 2002} WL 31063976 (9th Cir. 2002) (remanded for rehearing in Doe v. Unocal Corp., 2003 WL 359787 (9th Cir. 2003)).

military which had directly imposed the conditions. The plaintiff's suit could proceed under the ATCA because Unocal knowingly provided practical assistance which substantially enabled the abuses. Unocal stands for the proposition that private multinational corporations can be held liable in American courts for human rights abuses committed in foreign countries, even though these corporations have no direct connection to the abuses. American corporations that sell filtering software stand in a dangerous position after Unocal, as these corporations have provided China with the technology used to violate human rights.

As these cases show, private actors do not have to be direct agents of the state to be held liable under the ATCA. International law holds liable entities complying with abusive government rules, when these rules violate human rights norms. When a business invests in a state with a repressive government, such as China, it is often impossible for the business to avoid becoming complicit in human rights abuses. American ISPs cannot operate in China without pledging to follow China's strict filtering rules and face expulsion from the market as punishment. ISPs face the choice of either foregoing revenue from the second largest Internet market or agreeing to self-censor their Web content. Unfortunately, many corporations have opted to self-censor.

International legal standards suggest that these American corporations should refuse to provide equipment to China when it is known that the equipment will be used to abuse human rights. The UDHR preamble states that "every individual and every organ of society" should promote and secure the universal observance of the human rights contained within, including the freedom of speech and the freedom of access to information. Corporations, by their public nature and major presence, are surely organs of society. The International Covenant on Economic, Social and Cultural Rights ("ICESCR") preamble additionally acknowledges private human rights obligations: "Realizing that the individual, having duties to other individuals and to

^{107.} *Id.* at *24. The Ninth Circuit overturned the district court's decision to dismiss claims against Unocal because its conduct did not rise to the level of "active participation." *Id.* at *10.

^{108.} Id. at *10–15. The Myanmar military provided security and other services to aid in Unocal's pipeline project in Burma, with allegations that Unocal hired the military. Id. at *2. Plaintiffs allege that the military subjected them to a number of human rights abuses, including forced labor, rape, execution, and torture, and that Unocal had knowledge of these actions. Id. at *4. The district court held that such allegations did not rise to the level of "active participation" necessary to impose liability on Unocal under the ATCA, but the Ninth Circuit reversed, holding that by providing the military with photographs and maps indicating where to provide security and build infrastructure, Unocal gave the abusers enough practical assistance to hold the corporation liable. Id. at *14.

^{109.} Ratner, supra note 103, at 500-01.

^{110.} Beth Stephens, *The Amorality of Profit: Transnational Corporations and Human Rights*, 20 Berkeley J. Int'l L. 45, 51 (2002).

^{111.} *Id.* at 73 ("Certain international human rights prohibitions are triggered only with some level of state involvement or complicity."); Ratner, *supra* note 103, at 502.

^{112.} International Covenant on Economic, Social and Cultural Rights, G.A. Res. 2200A, U.N. GAOR, 21st Sess., Supp. No. 16, at pmbl, U.N. Doc. A/6316 (1966).

the community to which he belongs, is under a responsibility to strive for the promotion and observance of the rights recognized in the present Covenant." By recognizing these documents, members of the international legal system have come to the consensus that private corporations are liable for upholding human rights and under a duty to avoid violations. ¹¹⁴

Corporate liability for human rights abuses makes sense. Corporations are powerful and often necessary to the success of government suppression. China's Internet regulation system is successful because of American corporate aid. If ISPs refused to pledge compliance with the rules, China would be forced to seek other investors and would be pressured to rethink its regulations. Without American filtering software, China would either have to develop its own equipment or contract with other foreign corporations. If American companies set the precedent of noncompliance, other countries may follow, forcing China to choose between participation in the global economy or information "purity" within its borders.

Imposing civil liability on United States corporations which pledge conformity to China's regulations or which provide the Chinese government with filtering software will make China's surging Internet market less attractive to corporate fiduciaries. Companies involved in such business do insist they are innocent. Nortel spokeswoman Julie Kua admitted that the company sold its firewall products in Shanghai but said, "holding Nortel responsible would be like blaming Boeing for al-Qaeda flying its planes into the World Trade Centre," and added that Nortel sold its products with no knowledge as to how they would be used by the Chinese government. Her analogy fails. Boeing sold its planes to legitimate airlines. Nortel sold its products to a nation with the outspoken agenda of quashing the freedom of speech and the freedom of information access. Nortel should have known how China would use its software.

^{113.} Covenant on Civil and Political Rights, supra note 81, at pmbl.

^{114.} Although the liability of non-state actors is widely recognized, liability of corporations under the ATCA can take another route by finding corporations to be state actors. In *Beneal v. Freeport-McMoran, Inc.*, the court held that a corporation found to be a state actor could be held liable for human rights abuses that violate customary international law. 969 F. Supp. 362, 376 (E.D. La. 1997). Corporations that act in complicity with the state will be considered state actors. *See, e.g., id.* at 374–80; Kadic v. Karadzic, 70 F.3d 232, 245 (2d Cir. 1995); Doe. v. Unocal Corp., 963 F. Supp. 880, 890–91 (C.D. Cal. 1997) (courts apply the standards of domestic civil rights cases to determine the complicity of private actors). Again, American ISPs and software companies complying with China's promulgations and providing the necessary equipment would likely be considered state actors for purposes of the ATCA liability.

^{115.} Lee, *supra* note 10.

2. American Corporations Violating the ICCPR Should Be Liable Under the ATCA

ATCA liability attaches to corporations violating the "law of nations or a treaty of the United States." Considering the treaty provision as the first source of liability under the ATCA, the ICCPR was "consciously adopted as [a] legally binding [treaty]" by the United Nations General Assembly, open for ratification by the states. Because the ICCPR recognizes the duty of corporations to adhere to its provisions and is considered legally binding, American ISPs and software companies can be held liable for violating its provisions. Article 19 of the ICCPR states, "[e]veryone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers... through any... media." Therefore, American ISPs and software corporations complying with the Chinese speech and information restrictions by equipping the Chinese government with the means necessary to enforce these restrictions could be liable under the ATCA for violating a treaty to which the United States is a party.

The United States ratified the ICCPR on June 8, 1992. Liability under this provision is complicated by the fact that the United States Senate termed the ICCPR a "non-self-executing" treaty, meaning that its provisions do not have the force of domestic law until implementing legislation is passed. Some courts disregard treaty provisions under this arrangement, while others assume that non-self-executing treaties can have domestic effect. For instance, in *United States v. Toscanino*, the Second Circuit gave legal effect to non-self-executing treaties as evidence of binding principles of international law. This decision was later cited with approval by the *Filartiga* court.

Furthermore, scholars persuasively argue that the notion of non-self-executing treaties is unconstitutional. The concept of non-self-

^{116. 28} U.S.C. § 1350 (2000).

^{117.} Hurst Hannum, *The Status of the Universal Declaration of Human Rights in National and International Law*, 25 GA. J. INT'L & COMP. L. 287, 318 (1996). "The ICCPR is a signed, ratified treaty." Beharry v. Reno, 183 F. Supp. 2d 584, 595 (E.D.N.Y. 2002).

^{118.} See supra p. 505 and note 111.

^{119.} Covenant on Civil and Political Rights, supra note 81, at art. 19.

^{120.} Christopher L. Blakesley et al., Documentary Supplement to Cases and Materials on the International Legal System 533 n.1 (5th ed. 2001) [hereinafter Blakesley, Documentary Supplement].

^{121.} Beharry, 183 F. Supp. 2d at 593–95. Such treaties are termed "RUDs," signifying that the treaties have been ratified with attached "reservations, understandings, and declarations." *Id.* at 593.

^{122.} Id. at 594.

^{123.} See United States v. Toscanino, 500 F.2d 267, 278–81 (2d Cir. 1974).

^{124.} Filartiga v. Pena-Irala, 630 F.2d 876, 882 n.9 (2d Cir. 1980).

^{125.} Christopher L. Blakesley, Autumn of the Patriarch: The Pinochet Extradition Debacle & Beyond, 90 J. Crim. L. & Criminology 1 (2001), reprinted in Christopher L. Blakesley et al., The International Legal System: Cases and Materials 667 (5th ed. 2001) [hereinafter Blakesley, International Legal System].

executing treaties was judicially created, ¹²⁶ but Article VI of the Constitution states, "all Treaties made . . . under the Authority of the United States, shall be the supreme Law of the Land." Because the Constitution is the utmost source of law governing the United States, a plausible argument exists that non-self-executing treaties are unconstitutional in limiting the force of what the Constitution declared as supreme law. When the United States ratified the ICCPR, the ICCPR became binding law under the terms of the Constitution, and American corporations are thereby obligated to observe its provisions.

U.S. corporations that aid China in restricting the freedom of speech and the freedom of access to information via the Internet therefore directly violate Article 19 of the ICCPR. These freedoms under Article 19 are not absolute—the ICCPR limits restrictions to those that are provided by law, necessary for respect of the rights or reputations of others, and necessary for the protection of national security, public order, public health, or morals. When the United States ratified the ICCPR, it declared that the United States would not limit the right to free speech, and it urged other parties to the ICCPR to refrain from doing so as well.¹²⁹ China's Internet regulations deny its citizens categories of speech and information that go well beyond the scope of allowable restrictions. China's keyword method of regulating is overbroad. For example, tagging the word "breast" not only filters out pornography, which is an allowable restriction under the ICCPR, but it also denies access to Web sites containing information on breast cancer. Blocking information on breast cancer will not help protect national security, order, health, or morals. This is an unjustifiable restriction. Because U.S. corporations make the technology that imposes these restrictions, U.S. corporations may be liable to China's citizens for violations of Article 19 of the ICCPR.

3. The "Law of Nations" Should Be Extended to Include the Freedoms of Speech and Access to Information, and American Corporations Violating Those Rights Should Be Liable Under the ATCA

American corporations could also be liable if violations against free speech and free access to information are considered a violation of the law of nations, an alternative cause of action under the ATCA. The content of the law of nations can be determined by examining court decisions enforcing and explaining international law, the works of jurists,

^{126.} Id. at 669.

^{127.} U.S. CONST. art. VI, cl. 2.

^{128.} Covenant on Civil and Political Rights, supra note 81, at art. 19.

^{129.} See Ali Khan, A Theory of Universal Democracy, 16 Wis. Int'l L.J. 61, 113 n.92 (1997); David P. Stewart, U.S. Ratification of the Covenant on Civil and Political Rights: The Significance of the Reservations, Understandings and Declarations, 14 Hum. Rts. L.J. 77, 79–80 (1993).

and the general practice of nations.¹³⁰ Flouting established norms of international human rights is a violation of the law of nations.¹³¹ Courts must determine and interpret human rights law "as it has evolved and exists among the nations of the world today."¹³² Not all rights are actionable under the ATCA—only those rights sharing the general consent of nations.¹³³ Courts and jurists consider the ICCPR and the UDHR when ascertaining international human rights law; general assent among states favors the interpretation of these provisions as binding international law, and therefore the law of nations.

The United Nations General Assembly unanimously adopted the UDHR on December 10, 1948.¹³⁴ The UDHR was not enacted as a binding treaty, but instead served as a declaration of basic human rights principles to establish a common standard to be achieved by states for all individuals.¹³⁵ The General Assembly adopted the ICCPR on December 16, 1966, and on March 23, 1976, it entered into force.¹³⁶ Unlike the UDHR, the states consciously adopted the ICCPR as a legally binding treaty, open for ratification by the states.¹³⁷ As of 2001, there were 115 parties to the covenant.¹³⁸ States recognized the binding effect of the ICCPR provisions from the outset, but gradually the status of the UDHR has significantly evolved. The ICCPR constitutes customary international human rights law by its binding nature; courts, jurists, and states ascertaining international human rights law have also considered the UDHR as evidence of binding norms.

The UDHR, read in connection with the United Nations Charter, creates binding international law. The Restatement (Third) of Foreign Relations Law ("Restatement") recognizes that the UDHR provisions enumerate binding Charter principles, and it states, "the general pledge of members in the Charter... has been made definite by the Universal Declaration and that failure by any member to respect the rights recognized in the Declaration is a violation of the Charter." The Restatement also recognizes that the Charter, UDHR, other international resolutions and declarations, and the practices of states, all

^{130.} Sarei v. Rio Tinto, 221 F. Supp. 2d 1116, 1131 (C.D. Cal. 2002).

^{131.} Filartiga v. Pena-Irala, 630 F.2d 876, 880 (2d Cir. 1980).

^{132.} Beneal v. Freeport-McMeran, Inc., 197 F.3d 161, 165 (5th Cir. 1999); Kadic v. Karadzic, 70 F.3d 232, 238 (2d Cir. 1995); Filartiga, 630 F.2d at 881.

^{133.} Filartiga, 630 F.2d at 881. The court further noted that it is "only where the nations of the world have demonstrated that the wrong is of mutual, and not merely several, concern, by means of express international accords, that a wrong generally recognized becomes an international law violation within the meaning of the statute." *Id.* at 888.

^{134.} Blakesley, International Legal System, supra note 125, at 697.

^{135.} Marjorie M. Whiteman, 5 Digest of International Law 243 (1965) (internal citation omitted).

^{136.} Blakesley, DOCUMENTARY SUPPLEMENT, supra note 120.

^{137.} Hannum, supra note 117.

^{138.} Blakesley, DOCUMENTARY SUPPLEMENT, *supra* note 120.

^{139.} RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 701 Reporters' Note 4 (2002) [hereinafter RESTATEMENT]. *See also* Hannum, *supra* note 117, at 352–53 ("Legally and politically, it is the Universal Declaration of Human Rights which defines the Charter's human rights provisions.")

combine to create customary international law that requires states to abide by the UDHR provisions. In addition, the United Nations General Assembly declared that the Charter's human rights principles are embodied in the UDHR and constitute basic principles of international human rights law. Since nearly all states are members to the Charter, and the UDHR was passed without dissent, it is severally recognized that the provisions of the UDHR constitute international human rights law and, therefore, the law of nations.

Although the ICCPR and UDHR contain provisions establishing the freedom of speech and freedom of access to information, ¹⁴² the court in *Guinto v. Marcos* held that freedom of speech did not constitute a law of nations because it failed to rise to the level of universal recognition. ¹⁴³ The practice of other courts would argue otherwise. The court in *Filartiga* contemplated the United Nations Charter and stated that, since the inception of the ICCPR and UDHR, members of the United Nations have been fully aware of their human rights obligations under the Charter. ¹⁴⁴ When determining that torture violates the law of nations, the court considered the ICCPR and UDHR as obvious evidence of universal renunciation of torture. ¹⁴⁵ Similarly, courts today can consider the ICCPR and UDHR provisions as evidence of a universal renunciation of illegitimate restrictions of speech and access to information.

The International Court of Justice has consistently held without dissent that the UDHR is of sufficient legal status to justify its use by the Court when determining a state's obligations under international law. ¹⁴⁶ In each finding of a violation of a fundamental right, the justices have referred to the UDHR. ¹⁴⁷

Furthermore, jurists who contemplate the substance of international human rights law consider the UDHR binding. Although scholars acknowledge that the UDHR was first proclaimed as a common standard of achievement for all nations rather than a legally binding treaty, its status has considerably elevated over time. Many now argue that its

^{140.} RESTATEMENT, *supra* note 139. Section 701 of the Restatement references numerous United Nations resolutions and authoritative statements imposing duties on states to observe the UDHR provisions. *See id.*

^{141.} Filartiga v. Pena-Irala, 630 F.2d 876, 882 (citing G.A. Res. 2625 (XXV) (Oct. 24, 1970)).

^{142.} Covenant on Civil and Political Rights, *supra* note 81, at arts. 18, 19; Declaration of Human Rights, *supra* note 80, at arts. 18, 19.

^{143. 654} F. Supp. 276, 280 (S.D. Cal. 1986).

^{144. 630} F.2d at 883.

^{145.} *Id.* at 883–84. In considering the ICCPR and UDHR with regard to torture, the court stated, "we have little difficulty discerning its universal renunciation in the modern usage and practice of nations." *Id.* at 883.

^{146.} Hannum, supra note 117, at 338.

^{147.} Id.

^{148.} Whiteman, *supra* note 135, at 243 (noting that the Chairperson of the Commission, Eleanor Roosevelt, stated that the basic character of the document is not a treaty or international agreement and is only a declaration of the basic principles of human rights to be stamped with the approval of the General Assembly).

political authority is second only to that of the Charter, and "its reception at all levels has been such that, contrary to the expressed intention of its authors, it may have now become part of international law." Specifically, jurists consider the first twenty-one articles of the UDHR to be binding international law. In particular, the freedom of speech and the freedom of access to information are explicitly enumerated in Articles 18 and 19. Today, many scholars believe that the UDHR is binding international law on all states because of its prevalent recognition by many nations and its long-standing use as a declaration of human rights norms among numerous nations.

In addition to jurists, various international conferences have revealed that many organizations consider the UDHR to be obligatory upon states. The International Law Institute declared many years ago that the UDHR established an obligation on states to guarantee the human rights contained within. The International Law Association noted that the UDHR is universally regarded as an elaboration of the human rights provisions in the United Nations Charter, and perhaps all provisions in the UDHR are widely recognized as customary international law. The respect afforded the UDHR by these organizations illustrates the broad acceptance of its legitimacy in the international community.

^{149.} John P. Humphrey, *The UN Charter and the Universal Declaration of Human Rights, in* The International Protection of Human Rights 39, 51 (Luard ed., 1967), *reprinted in* Blakesley et al., International Legal System, *supra* note 125, at 699. *See also* Restatement, *supra* note 139, § 701 Reporter's Notes 4 & 6; Stephens, *supra* note 110, at 82.

^{150.} Philip Alston, *The Universal Declaration at 35: Western and Passé or Alive and Universal*, 31 INT'L COMMISSION JURISTS REV. 60, 69 (1982).

^{151.} Declaration of Human Rights, supra note 80, at arts. 18–19.

See supra notes 145-46 and accompanying text; John P. Humphrey, The International Bill of Rights: Scope and Implementation, 17 WM. & MARY L. REV. 527, 529 (1976). One of the principle drafters of the UDHR concludes that since its adoption, "the Declaration has been invoked so many times both within and without the United Nations that lawyers now are saying that, whatever the intention of its authors may have been, the Declaration is now part of the customary law of nations and therefore is binding on all states." Id.; see also Humphrey Waldock, Human Rights in Contemporary International Law and the Significance of the European Convention, 11 INT'L AND COMP. L.Q. 1, 15 (Supp. 1965) (widespread recognition of the provisions of the Declaration "clothes it . . . in the character of customary international law"); Louis B. Sohn, The Human Rights Law of the Charter, 12 TEX. INT'L L.J. 129, 133 (1977) (viewing the UDHR to be both an "authoritative interpretation of Charter obligations" and a "binding instrument in its own right"); PATRICK THORNBERRY, INTERNATIONAL LAW AND THE RIGHTS OF MINORITIES 237–38 (1991) (stating that the UDHR is "the most valid interpretation of human rights and freedoms which the Members of the United Nations pledge to promote"); A.H. ROBERTSON & J.G. MERRILLS, HUMAN RIGHTS IN THE WORLD 96 (3d ed. 1989) (the UDHR "by reason of its constant reaffirmation by the General Assembly and in numerous other texts . . . can . . . be taken as a statement of customary international law, establishing standards which all States should respect"); Richard B. Bilder, The Status of International Human Rights Law: An Overview, in INTERNATIONAL HUMAN RIGHTS LAW & PRACTICE 1, 8 (James Tuttle ed., 1978). Fernandez v. Wilkinson, 505 F. Supp. 787, 796 (D. Kan. 1980) (citing Bilder's conclusion that the "standards set by the Universal Declaration of Human Rights, although initially only declaratory and non-binding, have by now, through wide acceptance and recitation by nations as having normative effect, become binding customary law").

^{153.} Hannum, supra note 117, at 323.

^{154.} Id.

General assent among nations is evidenced by the unanimous passage of the UDHR, with no dissent, by the United Nations General Assembly. Additionally, 115 states signed the ICCPR. According to Galindo Pohl, a Special Representative of the United Nations Commission on Human Rights, the rights established by the UDHR have become customary international law through state practice and *opinio juris*—states respect the rights in the UDHR based on a sense of legal obligation ¹⁵⁵—and

[e]ven if the strictest approach is adopted to the determination of the elements which form international customary law, that is, the classical doctrine of the convergence of extensive, continuous and reiterated practice and of *opinio juris*, the provisions contained in the Universal Declaration meet the stringent standards of that doctrine.¹⁵⁶

A United States district court, in *Fernandez v. Wilkinson*, ¹⁵⁷ upheld the notion that the standards set by the UDHR have become binding human rights norms through the general assent of nations. ¹⁵⁸ A number of nations have publicly expressed the view that the UDHR is binding customary international law: Finland, Denmark, Iceland, Norway, Sweden, Uruguay, Mexico, Chile, Columbia, Venezuela, Nicaragua, Bolivia, the former Yugoslavia, Czechoslovakia, Azerbaijan, Australia, Senegal, United States, Canada, Guyana, Switzerland, Jordan, and Japan. ¹⁵⁹ Ample evidence suggests that the general assent of nations requirement has been satisfied, and that the provisions of the UDHR calling for the freedoms of speech and access to information are binding among states.

In summation, multinational corporations can be liable under the ATCA for violations of the freedom of speech and the freedom of access to information as guaranteed by the UDHR and ICCPR. The burden of proof in establishing customary norms in the field of human rights law has been met and surpassed. Consistent with the evolutionary nature of the law of nations, United States courts should open the door to Chinese citizens who seek to restrain American corporations from aiding the human rights oppressions in China.

^{155.} RESTATEMENT, supra note 139, § 701 cmt. c.

^{156.} Question of the Violation of Human Rights and Fundamental Freedoms in any Part of the World, Commission on Human Rights, 43d Sess., at 4, U.N. Doc. E/CN.4/1987/23 (1987).

^{157. 505} F. Supp. 787 (D. Kan. 1980).

^{158.} See id. at 796.

^{159.} Hannum, *supra* note 117, at 326–32. Finland has taken an extremely expansive view of the international human rights covenants, holding that even states that have not ratified them are bound by their provisions as United Nations Members. *Id.* at 326 n.162. In addition, the Yugoslav Constitutional Court stated that the UDHR and ICCPR express recognized norms of international law. Eyal Benvenisti, *Judicial Misgivings Regarding the Application of International Law: An Analysis of Attitudes of National Courts*, 4 Eur. J. INT'L L. 159, 165 n.28 (1993).

D. Recent Developments: The House of Representatives Passes Legislation to Fight for Internet Freedom

In early October 2002, United States Representative Christopher Cox authored a bill, widely supported in the House of Representatives and Senate, which fights state-sponsored Internet jamming. According to Cox, the "freedom of expression has grown with the expansion of technology The success of U.S. policy in support of freedom of speech . . . requires new initiatives to defeat totalitarian controls over the Internet." On July 16, 2003, the House passed Cox's legislation, known as the "Global Internet Freedom Act" ("Act"). 162

The Act demonstrates the connection between the liberating cyberworld and the newly evolved ideals of global free speech and global access to information. The Act references the UDHR's provision guaranteeing the freedom to receive and disseminate ideas via any medium and calls upon the United States to defeat oppressive Internet regulations in other nations. The Act proposes to establish the Office of Global Internet Freedom and to allocate it \$50,000,000 in 2003 and 2004 to combat state-sponsored Internet control by providing Chinese citizens, among others, with the software to evade government restrictions. The Act further instructs the United States to publicly and consistently renounce governments that restrict the Internet and to submit a resolution to the United Nations Human Rights Commission condemning all governments that censor the Internet. In the words of Representative Cox, "the precious freedoms of speech and press in the American Constitution... are not special privileges to which only Americans are entitled."

IV. RECOMMENDATION

As the leading democratic nation, the United States has a strong commitment to upholding human rights. *Beharry v. Reno* held that the nation's credibility would be weakened by tolerating non-compliance with international human rights norms and treaties and by avoiding

^{160.} Paul Wilson, Censorship Collides With Free Enterprise, ORANGE COUNTY REGISTER, Oct. 2, 2002, available at 2002 WL 5461594. Cox, the House Policy Chairman, introduced the bill together with Tom Lantos (D-CA), a ranking member of the House International Relations. Senators Ron Wyden (D-OR) and John Kyl (R-AZ) introduced the bill to the Senate. Press Release, Sen. Ron Wyden, Wyden, Kyl Fight Web Censors with Global Internet Freedom Act (Oct. 10, 2002), at http://wyden.senate.gov/~wyden/media/2002/2002A11719.html.

^{161.} Press Release, U.S. House of Representatives Policy Committee, Bill Proposes Global Strategy Against Internet Jamming (Oct. 4, 2002), 2002 WL 101226428.

^{162.} Press Release, Federal Document Clearing House, House Passes Global Internet Freedom Bill Will Protect Human Rights Abroad (July 16, 2003), 2003 WL 101226428 [hereinafter Internet Freedom Bill].

^{163.} Global Internet Freedom Act, H.R. 5524, 107th Cong. §§ 2, 4 (2002).

^{164.} Id. § 4.

^{165.} Id. § 5

^{166.} Internet Freedom Bill, supra note 162.

enforcement of these same norms within its own borders.¹⁶⁷ The United States

cannot expect to reap the benefits of internationally recognized human rights—in the form of greater worldwide stability and respect for people—without being willing to adhere to them itself. As a moral leader of the world, the United States has obligated itself not to disregard rights uniformly recognized by other nations. ¹⁶⁸

It would be hypocritical for the United States to allow technology companies and ISPs within its borders to aid in the violation of human rights in China. Representative Cox's bill, if enacted, would provide Chinese citizens with an Internet escape route by supplying them with the necessary technology and materials, but American corporations fighting on China's side could nullify these efforts.

Cox's ideas would however, impose American free speech standards on states with very different political ideologies. The United States, acting as "an arbiter of what sort of control is acceptable online," would be ignoring international notions of sovereignty and comity. Although the freedom of speech and the freedom of access to information as enumerated in the UDHR and ICCPR are extensively recognized, the degree of permissible censorship varies from state to state. To

Radical cultural relativists hold that human rights standards differ among states, so what may be lawful in one culture should not be imposed on another.¹⁷¹ The view of weak cultural relativists is more fitting to the international human rights scenario—it maintains the universality of human rights norms, but holds that these norms are "subject to secondary cultural modifications."¹⁷² The United States should not provide Chinese citizens with evasive software technology as called for by Cox's bill, as this would completely disrespect China's right as a sovereign to formulate its own censorship standards, no matter how repugnant these standards may be to the United States. Because China's regulations rise above mere "cultural modification" and amount to human rights abuses, the United States instead should prevent American corporations from assisting Chinese censorship. The United States has the power to forbid its corporations from participating in human rights

^{167.} Beharry v. Reno, 183 F. Supp. 2d 584, 601 (E.D.N.Y. 2002).

^{168.} *Id*.

^{169.} Bill Thompson, America Bids to Become Net Watchdog, BBC News, at $\text{http://news.bbc.co.uk/2/hi/technology/2299259.stm} \ (\text{Oct. 4, 2002}).$

^{170.} For example, in some countries, pictures containing nudity are illegal and socially unacceptable; in others, they are a cultural norm. *Id.*

^{171.} GREGORY J. WALTERS, HUMAN RIGHTS IN AN INFORMATION AGE 248 (2001).

^{172.} *Id.* at 249. The weak cultural relativists take a position that human rights are a radically new concept in history, and "[c]ommunitarian societies that give ideological and practical priority to the community over the individual are antithetical to the implementation and maintenance of human rights." *Id.* at 250.

abuses.¹⁷³ The United States needs to end American involvement in China's Internet regulatory system by holding ISPs and technology corporations liable under the ATCA. This would enable the United States to balance its liberal views on human rights with its respect for China's sovereignty.

To fulfill the ATCA's requirements, courts should find that the ICCPR constitutes a binding treaty, notwithstanding its non-self-executing status, or courts should extend the law of nations to include the freedom of speech and the freedom of access to information. Imposing liability on these multinational corporations will not only sever critical aid to China's success at censorship, but it will also send a message that the United States, as a nation and not merely a government, will take no part in denying fundamental rights to citizens of a free world.

Representative Cox's bill does propose the entirely reasonable action of calling for the United Nations' support in condemning governments that suppress the freedom of speech and the freedom of access to information on the Internet. A resolution would not only validate the United States' position, but it would substantially impede China from obtaining any assistance from foreign ISPs or software companies, as states will likely comply with the resolution. Since China is a member state, it will feel greater pressure to effectuate the human rights contained in both the UDHR and ICCPR in cyberspace. Holding American corporations liable for their involvement in enforcing the regulations would be a more effective—and subtler—response to China's repression compared to Cox's idea of active intervention. It would also be easier for the international community to accept.

V. CONCLUSION

To feel the freedoms of democracy for one day, all one needs is a username and a password. Without government-imposed censorship, the possibilities for communication and information exchange are boundless between citizens of a free world. China's regulations overstep the bounds of protective limitation and intrude on the freedoms of all its citizens. By controlling what its citizens can say and see, China can rewrite and disguise its history and completely inhibit social change. For example, China deliberately installed the keywords "Tiananmen" and "human rights" onto its filtering software to destroy user access to Web pages containing these topics. As commentators have noted, "[w]hoever controls language controls a society's memory." 176

^{173.} Stephens, supra note 110, at 60.

^{174.} Global Internet Freedom Act, H.R. 5524, 107th Cong. § 5 (2002).

^{175.} Rowan Callick, Software Aids China's Censors: Amnesty, Austl. Fin. Rev., Dec. 3, 2002, at 12, 2002 WL 26291439.

^{176.} Kenneth Neil Cukier, *Don't Let Governments Politicize the Internet*, ASIAN WALL. ST. J., Nov. 5, 2002, at A9, 2002 WL-WSJA 23020309.

With the advancement of the Internet, China faces more knowledgeable and globally aware citizens. To enhance its economy, China continues to invest billions of dollars in building modern telecommunications, resulting in millions of new Internet users each year.¹⁷⁷ Contrary to this expansion of information access, the Chinese government strictly controls its citizens by blocking access to broadly-"sensitive information" categories of and expression." Penalties for violating the regulations are severe—citizens have been sentenced up to twelve years in prison for offenses such as posting pro-democracy material and articles informing citizens of Red Cross medicine sales on the Internet. ¹⁸⁰ As of late November 2002, Amnesty International lists thirty-three Chinese "prisoners of conscience" jailed for using the Internet to access or disseminate information; of those prisoners, three have died in custody. Two of the prisoners reportedly died from torture. 182

The freedom of speech and expression contained in the First Amendment remain a sacred tradition in the United States. At a minimum, the United States should guarantee that its government, corporations, and citizens refrain from interfering with these freedoms in cyberspace. Many Chinese citizens, seeking the same freedoms, have signed the Declaration of the Independence of Cyberspace to evidence their dedication to making the Internet a free forum for all and to create a society where they are guaranteed their fundamental human rights. Through the Declaration, the Internet users of China proclaim:

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.... We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts. We will create a civilization of the Mind of Cyberspace. May it be more humane and fair than the world your governments have made before. 184

May the United States and the international community answer their plea.

^{177.} SARS in China, supra note 16.

^{178.} Id.

^{179.} Callick, supra note 175.

^{180.} TEAR DOWN THIS FIREWALL, *supra* note 36.

^{181.} Press Release, Amnesty International, Amnesty International Report: Deadly Web—China's Internet Users at Risk of Arbitrary Detention, Torture, and Execution (Nov. 26, 2002), available at http://www.amnestyusa.org/news/2002/china11262002.html.

^{182.} Id.

^{183.} Barlow, supra note 1.

^{184.} Id. (emphasis added).