

SYRACUSE UNIVERSITY LAW & TECHNOLOGY JOURNAL

Technological Software That Counters Internet Jamming: Its Role in the U.S. and In
Non-Democratic Countries

Philip J. Oliveri

Fall 2003

INTRODUCTION

There is virtually 10% of the world's population using the Internet, and more are gaining access each day.¹ The Internet has become a powerful engine and tool for democratization (through e-governance) and economic expansion (through e-commerce), which is greatly facilitated by the free exchange of ideas and information over the World Wide Web.² Technological and economic developments may well widen the usage of the Internet by reducing costs and simplifying technical skills.³ The Internet and other digital technologies may serve to strengthen the establishments of civic society, widening the prospects of information, communication, and participation in the electronic public sphere, and allowing well-organized civil social groups to flourish economically and politically.⁴ Yet there are authoritarian governments that consider the Internet as being subversive, and as a result, they aggressively block and censor its use by their citizens. These efforts can be seen as restricting an individual's freedom to receive and exchange

¹ The House Policy Committee, *Establishing Global Internet Freedom: Tear Down This Firewall*, available at http://policy.house.gov/html/news_item.cfm?id=112.

² *Id.*

³ PIPPA NORRIS, DIGITAL DIVIDE, 92 (2001)..

⁴ *Id.* at 172.

information, which, under democratic countries' standards, is considered to be an implicit right for every person.

The United States has a strong interest in expanding the scope of accessibility of the Internet on a global scale because of the economic and political benefits involved. For instance, the U.S. gross domestic national product and investments in U.S. biomedical companies can increase exponentially.⁵ This is attributed to the advantages of the Internet: it provides a cost effective means of both communication and information management.⁶ Moreover, the U.S. maintains a foreign policy that supports the universal human rights of freedom of speech, press, and association, as stated under the Universal Declaration of Human Rights.⁷ By upholding this Declaration, the U.S. global presence and its political influence may be strengthened. Thus, in order to defend and promote their economic interests, as well as the essence of global freedom, the United States has introduced a bill designed to fight foreign Web censorship.⁸ It would create an Office of Global Internet Freedom that would develop and promote anti-blocking technology directed towards authoritative governments that restrict their citizens' access to the Internet.⁹ Hence, this would initiate a proliferation of anti-blocking software products designed to circumvent filters and firewalls both abroad and in the United States.

⁵ See *U.S. Investment in China Worsens Trade Deficit*, available at <http://www.epinet.org/briefingpapers/FDI/fdi.htm>.

⁶ John H. Taylor III, *The Internet in China: Embarking on the "Information Superhighway" With One Hand on the Wheel and the Other Hand on the Plug*, 15 DICK. J. INT'L L. 621, 625 (1997).

⁷ See *Universal Declaration of Human Rights* available at <http://www.un.org/Overview/rights.html>.

⁸ Lisa M. Bowman, *Bill Aims at Foreign Web Censorship*, available at http://www.unpan.org/information/WorldGovernanceWatch/News2002-10_files/governance-10.htm#PPGAM04.

⁹ *Bipartisan, Bicameral Bill Stops Internet Jamming*, available at http://policy.house.gov/html/news_release.cfm?id=111.

However, this presents two dilemmas: one, limited support for U.S. intervention in foreign states, both domestically and internationally; and two, a clash between U.S. efforts to protect children from obscene material on the Internet and attempts to thwart state-directed Internet jamming.

THE ROLE OF TECHNOLOGY THAT COUNTERS INTERNET JAMMING IN FOREIGN COUNTRIES

The Internet is so large, so powerful, and so overwhelmingly efficient that it has become understood to be an integral aspect of politics, economics, and culture. Consequently, as the twenty-first century progresses in the midst of this Internet phenomenon, the global interest in the Internet is skyrocketing. Although the origins of the Internet are found in ARPANET, a computer network created by the United States in September of 1969 with the task of mobilizing research resources,¹⁰ the Internet is popular in Europe and Asia due to its ability to expose a user to a plethora of political, economic, and recreational sites.¹¹ The governments and private businesses in these countries are fervently developing telecommunication infrastructures “which will make the Internet universally accessible and affordable.”¹²

These efforts of universal accessibility, however, are in direct conflict with a number of national governments that have undertaken efforts to regulate the use and content of the Internet.¹³ They are motivated by different cultural, political, and religious

¹⁰ MANUEL CASTELLS, *THE INTERNET GALAXY*, 10 (2001).

¹¹ Michael Neubarth, *The Internet: A Global Look*, INTERNET WORLD, Nov. 1995, at 95.

¹² Taylor III, *supra* note 6, at 621.

¹³ *Id.*

concerns that are likely to threaten the development of a globally-networked and universally accessible Internet community.¹⁴ As a result, this would menace the potential economic rewards the Internet could foster for many countries through electronic commerce and joint investing. For instance, *Business Week* estimates that electronic commerce could boost the U.S. gross domestic product \$10-20 billion by the end of 2002.¹⁵ However, this depends on how well-exposed U.S. sites are in foreign countries. Therefore, several countries (the most proactive being the United States) are responding to these national governments' regulations in order to promote increased global accessibility to the Internet.

THE WAYS AUTHORITARIAN GOVERNMENTS INTERFERE WITH THEIR CITIZENS' INTERNET ACCESS

The Internet has the remarkable ability of disseminating and sharing information instantly and efficiently. Therefore, many nations are eager to take advantage of the Internet and the wealth of opportunities it offers. On the other hand, many national governments have imposed limitations on the accessibility of many sites and, in effect, the concepts of individual speech and expression are in jeopardy.¹⁶ For example, China is one nation which has traditionally kept the distribution of information and freedom of expression to a minimum.¹⁷ These efforts are attributed to maintaining political stability and avoiding any Western thought that would induce a potential overthrow of the

¹⁴ Taylor III, *supra* note 6, at 621.

¹⁵ LESLIE DAVID SIMON, NETPOLICY.COM, 35 (2000).

¹⁶ See Taylor III, *supra* note 6, at 622.

¹⁷ *Id.*

People's Republic of China.¹⁸ Other authoritative governments that utilize similar methods as China does are Burma, Cuba, Laos, Saudi Arabia, Iran, North Korea, Syria, Tunisia, Vietnam, and Yemen.¹⁹ All of the governments that restrict Internet access and/or block specific sites are non-democratic, and are using methods of control that include denying their citizens access to the Internet, censoring content, banning private ownership of computers, and making e-mail accounts so expensive that ordinary people cannot use them.²⁰ These countries utilize firewalls, filters, and other devices to block and censor the Internet.²¹ These are the most common ways in which authoritarian governments interfere with their citizens' access to the Internet:

Prevention of Internet Access

Many governments in the Middle East and Asia retain monopoly control of Internet Service Providers (ISPs)²² through state control of their country's telecommunications systems.²³ This monopoly supremacy enables these governments to enforce restrictive policies over the people's access to the Internet.²⁴

¹⁸ See Taylor III, *supra* note 6.

¹⁹ The House Policy Committee, *supra* note 1.

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

²³ *Id.*

²⁴ *Id.*

For example, the Syrian government attempts to block access to servers that provide free e-mail services.²⁵ According to the U.S. State Department, foreign diplomats have had their telephone service disrupted because the lines were used to access Internet providers outside the country.²⁶ Additionally, in Cuba, the Castro government controls and limits all Internet access, thereby ensuring that the Internet can only be accessed through government approved institutions.²⁷

Censorship of Internet Subject Matter

Among the most austere enforcers of Internet censorship are Bahrain, China, Iran, Kuwait, Saudi Arabia, Vietnam, and Yemen, each of which actively blocks web sites for execution of government goals and ambitions.²⁸ These governments often claim that censorship is necessary in order to protect public morality; however, in each case the government clearly intends to stifle potential political dissent and opposition.²⁹

Censorship is typically performed by employing the use of proxy servers.³⁰ By interposing the proxy server between the end user and the Internet (a task that is more feasible when the Internet Service Provider (ISP) is the government or a governmentally-controlled monopoly) the government can filter and block content.³¹ “In countries where

²⁵ The House Policy Committee, *supra* note 1.

²⁶ *Id.*

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.*

³⁰ Taylor III, *supra* note 6, at 637.

³¹ *Id.*

individual access to the Internet is rare, government agents are assigned to monitor activity at Internet cafes, literally watching what sites customers visit.”³² However, when unapproved Internet use is recurrent, Internet cafes will be closed. In Saudi Arabia, for example, the government has closed a number of Internet cafes, especially those established for women which have been specifically targeted as being used for “immoral purposes.”³³

Prohibiting Computer Ownership

The most striking limit on Internet use is achieved by government bans on personal computer ownership. In North Korea, Dictator Kim Jong-II has forbidden all Internet connections to the exterior of the country, thereby rendering North Korea as the only country where the Internet does not exist.³⁴ In March 2002, Castro’s government banned the sale of personal computers to the general public.³⁵ Government decree 383/2001 bans the sale of “computers, offset printer equipment, mimeographs, photocopiers and any other mass printing medium” to “associations, foundations, civic and non-profit organizations and Cuban private individuals.”³⁶

³² The House Policy Committee, *supra* note 1.

³³ *Id.*

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.*

Implementation of an E-mail Account Tax

In Cuba, only 60,000 of the country's 11 million people have Internet access.³⁷ This low number is directly correlated to the Castro government's high taxes on e-mail accounts,³⁸ where the e-mail registration tax is \$240 (in a country with a per capita income of \$1700)³⁹ Hence, such prohibitively high taxes are an effective means of ensuring that only a small minority have the capability to use the Internet.

U.S. RESPONSE TO AUTHORITATIVE GOVERNMENTS' RESTRICTIONS TO INTERNET ACCESS

On October 2, 2002, bipartisan, bicameral legislation was introduced in order to counter global Internet jamming and blocking.⁴⁰ House Policy Committee Chairman Christopher Cox (R-CA) and House International Relations Committee Ranking Member Tom Lantos (D-CA) introduced the legislation in a bipartisan effort, with Congressman Lantos stating that "the development and implementation of technologies to defeat Internet jamming and censorship are a logical next step in the struggle to defend human rights abroad."⁴¹ The two primary objectives of the bill, as delineated by the House Policy Committee, are to first develop and implement a global strategy to combat state-directed Internet jamming, and thereafter establish the Office of Global Internet Freedom, which would develop and implement technologies to defeat Internet jamming and

³⁷ The House Policy Committee, *supra* note 1.

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ Bowman, *supra* note 8.

⁴¹ *Bipartisan, Bicameral Bill Stops Internet Jamming, supra* note 9.

copyright.⁴² Although this legislation is intended to be directed towards all of the authoritative governments that restrict Internet access, its main target is China, due to the potential for economic opportunities involved and its long history of human rights violations.⁴³ For instance, several international firms are investing in the development of infrastructure projects in China in anticipation of a booming market of consumers of electronic industry products and services.⁴⁴ Moreover, its enormous market has the potential and capability to become an extremely valuable resource, both domestically and for the world as a whole.⁴⁵

However, there is limited support on both the domestic and international fronts for such U.S. intervention because the U.S. has the duty to respect state sovereignty, regardless of ideological clashes and differences.⁴⁶ Yet, although such dissent may impede the bill's progress, it seems that it will only do so momentarily and will nonetheless pass. This is based upon the underlying principle that as the overseer of international relations, the U.S. should intervene. Subsequent to its passage, the legislation will undoubtedly be successful in expanding the scope of global Internet access, especially in countries where the legislation is directed.

First and foremost, the United States finds its legitimacy to intervene in these countries based upon economic incentives. Not only will such restricted Internet access

⁴² *Bipartisan, Bicameral Bill Stops Internet Jamming*, *supra* note 9.

⁴³ *See id.*

⁴⁴ Taylor III, *supra* note 6, at 631.

⁴⁵ Ewan W. Rose, *Will China Allow Itself to Enter the New Economy?*, 11 DUKE J.COMP. & INT'L L. 451, 463 (2001).

⁴⁶ *See* Bowman, *supra* note 8.

adversely affect the United States' economic opportunities (i.e., limited global presence of U.S. Internet service providers), but it will also affect the opportunities for other countries as well, including the authoritative regimes themselves.⁴⁷ For instance, the Chinese government has implemented new Internet regulations that limit foreign investment in technology companies.⁴⁸ These new regulations are bound to cause concern among members of the Chinese IT community because such technology companies heavily depend on financial support from external investors.⁴⁹ Foreign investors will lose faith and confidence in the Chinese market, discouraging investment. Hence, the U.S. legislation intends to eradicate such financial discouragement that is sparked by the Chinese regulations of the Internet. This will placate some international opposition to the bill because the legislation will have positive economic rewards for countries such as Great Britain, Sweden, Germany, and Japan, who all have technological interest not only in China, but in other non-democratic countries as well.

Articles 9, 11, and 13 of the Chinese Internet regulations declare that service providers are liable for message content.⁵⁰ This new liability affects business in three ways. First, companies seeking to provide online service to Chinese citizens will be in a difficult position because it will be arduous, if not impossible, to monitor millions of daily electronic transmissions for improper message content.⁵¹ Second, numerous United

⁴⁷ Olaf Juptner, *Increased Regulation for Chinese Internet Use*, available at <http://www.e-gateway.net/infoarea/news/news.cfm?nid=1068>.

⁴⁸ *Id.*

⁴⁹ *See id.*

⁵⁰ Scott E. Feir, *Chinese Regulations Restricting Internet Access*, 6 PAC. RIM. L. & POL'Y J. 361, 382 (1997).

⁵¹ *Id.*

States companies, already engaged in business in China, are now vulnerable to government sanctions.⁵² These companies have little information available to help evaluate their risk exposure and avoid sanctions; therefore, this would dissuade these companies from integrating their businesses within China. Finally, foreign computer service providers are delaying entry into China because of the uncertainty created by the regulations.⁵³ One American biomedical company, disturbed over the restrictive nature of the regulations, is hesitant about conducting further use of the Internet in China. If the regulations are not rescinded, the company is planning to boycott all business relations with China.⁵⁴ Furthermore, U.S. and foreign businesses operating or providing Internet service in China must be willing to deal with unpublished rules⁵⁵ because the State Council Economic Leading Group is authorized to consistently add additional rules.⁵⁶ Thus, businesses involved in legal disputes with Chinese authorities and the government will be in a disadvantageous situation because of the difficulty of not having access to all relevant law regarding liability for message content.

Additionally, governmental censorship and control will slow the development of global Internet access. The censorship of the Internet may create political tensions with other nations, thus hindering foreign investment. Furthermore, companies which face political pressure at home to not engage in business that assists a nation in restricting free

⁵² Feir, *supra* note 50, at 383.

⁵³ *Id.*

⁵⁴ See David G. Anast, *Don't Throw Our Chinese Clients in Jail, Using the Internet is Not a Crime*, BIOMEDICAL MKT. NEWSLETTER, Vol. 6 No. 2, Feb. 1, 1996.

⁵⁵ See *id.*

⁵⁶ *Id.*

speech and expression are in the “unenviable position of choosing between abandoning the Chinese market or becoming a partner in the suppression of political dissent.”⁵⁷ As a result, this predicament would deter ISP’s from providing tools that would not only retard the development of China’s Internet, but also hinder progression towards universal accessibility to the Internet.⁵⁸

Finally (and probably the most legitimate argument to allow this legislation to come into effect), the regulations violate the spirit of Article 19 of the Universal Declaration of Human Rights, which was established on December 10, 1948 by the General Assembly of the United Nations.⁵⁹ It declares that, “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”⁶⁰ Although China has generally disregarded human rights,⁶¹ China cannot evade them anymore as it expands foreign commerce and encounters international law containing human rights provisions. Additionally, the Internet regulations treat the Chinese Constitution, as which provides that citizens have the “freedom of speech, press, assembly, association, process, and demonstration,” as essentially non-existent.⁶² Eventually, other countries will become involved in order to protect their political and economic interests, as well as those of the Chinese citizenry.

⁵⁷ Taylor III, *supra* note 6, at 640.

⁵⁸ Feir, *supra* note 50, at 383.

⁵⁹ *See supra* note 7.

⁶⁰ *See id.*

⁶¹ *See supra* note 47.

⁶² Feir, *supra* note 50, at 385.

U.S. foreign intervention has been and can now be validated pursuant to its traditional stance as being protective of global human rights. U.S. policy in support of freedom of speech, press, and association, aimed at defeating totalitarianism, has been successful.⁶³ According to Congressman Lantos, the legislation is a “logical next step in the struggle to defend human rights abroad.”⁶⁴ However, the proposed bill does place limits upon itself in regards to how far it can reach.⁶⁵ It states that “nothing in this Act shall be interpreted to authorize any action by the United States to interfere with foreign national censorship for the purpose of protecting minors from harm, serving public morality, or assisting with legitimate law enforcement aims.”⁶⁶

HOW THE TECHNOLOGY WORKS

One of the most important policies the proposed legislation possesses is the establishment of the Office of Global Internet Freedom, which will deploy technology that will counter Internet jamming.⁶⁷ The bill would allocate fifty million dollars every year for the next two years in order to aid the private sector in developing and promoting the anti-blocking technology.⁶⁸ These technologies incorporate proxy servers and encryption, which are the capability of bypassing the states’ attempts to restrict citizens’

⁶³ THE HOUSE POLICY COMMITTEE, *supra* note 9.

⁶⁴ *Id.*

⁶⁵ See, Euromole, *Jamming on the World Wide Web*, available at <http://www.theinquirer.net/?article=7144> (Jan. 10, 2003).

⁶⁶ *Id.*

⁶⁷ Bowman, *supra* note 8.

⁶⁸ Bowman, *supra* note 8.

Internet use.⁶⁹ It is imperative that the Office of Global Internet Freedom procures the aid of the private sector and obtains this technology in order to defeat Internet censorship. Such technology includes Triangle Boy, DynaWeb, SafeWeb, and Peek-a-Booty⁷⁰ which is already being used in many of the aforementioned non-democratic countries. In China, for instance, Triangle Boy has been successful in allowing Chinese citizens to surf the Web safely; in fact, over 100,000 hits per day.⁷¹ Unfortunately, its funding has expired,⁷² and using money allocated within the proposed bill is the only likelihood it has to reach Chinese users once again.

“The concept behind [this technological software] is simple: bypass the firewalls by providing an alternate intermediary to the World Wide Web.”⁷³ This software is operated by “global-thinking, local-acting” people in countries that do not censor the Internet (i.e., the United States).⁷⁴ A user in a country that censors the Internet (i.e., China) connects to the ad hoc network of computers running the software, such as Peek-a-booty.⁷⁵ However, the users in the countries that censor the Internet do not necessarily need to install any software.⁷⁶ They are merely make a simple modification to their Internet settings so that their access to the World Wide Web is mediated by the

⁶⁹ *Id.*

⁷⁰ THE HOUSE POLICY COMMITTEE, *supra* note 27.

⁷¹ *Id.*

⁷² *Id.*

⁷³ See *About the Peek-a-Booty Project (The concept and the code)*, available at <http://www.peek-a-booty.org/pbhtml/modules.php?name=Content&pa=showpage&pid=1> .

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ *Id.*

software's network.⁷⁷ The installation of the software simply makes the process of connecting to the Internet easier.

Next, randomly selected computers in the network retrieve the Web pages and relays them back to the user.⁷⁸ In regards to the censoring firewall, the user is essentially accessing a computer that is not included on its "banned" list. Then, the retrieved Web pages are encrypted utilizing a de facto standard for secure transactions as a way to thwart the firewall from examining the Web pages' contents.⁷⁹ Since the encryption being used is a secure transaction standard, it will seem like an ordinary e-business transaction to the firewall.⁸⁰

Thus, this software takes advantage of three aspects that enables it to operate efficiently and effectively. First, technologically efficient and fast computers, as well as Internet connections, are becoming increasingly available at affordable prices. The speed at which ordinary computers can process information and access the Internet enables people to run Web servers on their home computers and home broadband connections in a feasible manner.⁸¹

Secondly, national firewalls do allow partial access to the Internet; otherwise it would be harmful to a country's economic and technological welfare to block out the Internet entirely. Hence, firewalls prevent access only to Internet addresses that appear

⁷⁷ *About the Peek-a-Booty Project, supra* note 73.

⁷⁸ *Id.*

⁷⁹ *Id.*

⁸⁰ *Id.*

⁸¹ *Id.*

on their “banned” lists.⁸² A government running a firewall would need prior notification or knowledge of a Web site that possessed content the government did not desire their citizens to see. Consequently, pursuant to this knowledge or notification, the government would then be able to add it to the list. A government would most likely be aware of high-profile sites managed by large media organizations and human rights groups. It may also be aware of lesser-known sites, such as those managed by former citizens living in exile⁸³ (Taiwanese revolutionaries in China, for instance). However, it is unlikely that they would block access to an Internet address of a home computer they are not familiar with, such as a for-profit organization that uses encryption software that counters Internet jamming.⁸⁴ This software is classified as a *distributed* or *peer-to-peer* application.⁸⁵ What this means is that its efforts are the product of several computers working collectively as a collaborative network rather than a single computer accomplishing most of the labor. The dispersed nature of the software makes it more difficult for a hostile government to shut it down.⁸⁶ Given enough users, it would be virtually impossible to block access to or disable every computer in a network. Each computer in the network recognizes only a small number of computers in the network.⁸⁷ This makes it much more difficult for an unreceptive government to detect the Internet addresses of networked machines and consequently add them to their “banned” lists.

⁸² *About the Peek-a-Booty Project, supra* note 73.

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ *Id.*

⁸⁶ *Id.*

⁸⁷ *Id.*

Finally, citizens from a plethora of countries have embraced the philosophical notion of “thinking globally and acting locally.” What this means is that entering into the twenty-first century, people are more concerned about matters beyond their home front, such as the environment and human rights issues. Thus, they are giving to charities, taking part in demonstrations and contributing to activist organizations.⁸⁸ Therefore, this technological software will have the support from a morally conscientious, global human body.

HOW THIS U.S. LEGISLATION CAN SUCCEED

As previously mentioned, the establishment of the Office of Global Internet Freedom and its role in developing and deploying the technological software necessary to counter Internet jamming is the most important feature of the legislation.⁸⁹ Nonetheless, new technologies emerge on a regular basis, thereby making control difficult. Additionally, attaining the goal of permanently eradicating Internet jamming will prove challenging because of the emergence of these new and efficient technologies. Although the software that counters Internet jamming is wholly necessary in the battle against Internet jamming, it is not the ultimate solution. Congress and the Executive Branch must bring pressure from other democratic countries upon these authoritative regimes (which are responsible for Internet jamming and violating human rights) through other methods as well.

⁸⁸ *About the Peek-a-Booty Project*, *supra* note 73.

⁸⁹ *See* Bowman, *supra* note 8.

The most important technique in which to obtain legitimacy and to also gain support from other countries, is stressing the notion that these authoritative regimes are violating human rights. Therefore, submitting a resolution at the U.N. Human Rights Commission's annual meeting in Geneva would accomplish this goal.⁹⁰ This resolution should condemn all nations practicing Internet censorship, and declare that the democratic nations of the free world will aggressively protect the human rights of freedom of speech, expression, and information. Moreover, the resolution should contain a formal declaration which states that all people have the right to communicate freely with others on the Internet.⁹¹ In this manner, most democratic countries with an economic and political interest in protecting and expanding the universal accessibility of the Internet will be inclined to help bring more pressure upon the authoritative regimes. The best way to accomplish this is directing substantial international broadcasting resources that denounce restriction of the Internet. It would be most effective if it is achieved on a global level.⁹²

However, the U.S and other democratic nations may not need to exert themselves in order to accomplish these goals because the authoritative regimes' Internet regulations being self-defeating. This is because the filtering software used to censor subversive sites lacks accuracy when evaluating material.⁹³ First, a broad filtering protocol may mistakenly block helpful and important information, frustrating users by preventing

⁹⁰ THE HOUSE POLICY COMMITTEE,*supra* note 1.

⁹¹ *Id.*

⁹² *Id.*

⁹³ Feir,*supra* note 50, at 369.

access to legal and morally acceptable material.⁹⁴ As a result, this frustration could lead to either reconstructing the filtering system or removing it all together. Secondly, despite the authoritative governments' attempts to restrict Western news agencies and cultural sites, much of Western information still remains accessible.⁹⁵ Determined computer users continue to find ways to obtain this restricted, Western information. Thirdly, there are organizations that are devoted to maintaining the free exchange of ideas over the Internet.⁹⁶ For example, the creators of the Peek-a-Booty software have already initiated a series of networks that are helping Chinese and Middle Eastern Internet users bypass the restricted and blocked sites.⁹⁷ For instance, there are individuals that help subvert official control and protect the interests of free speech by posting material (which is banned to users in one part of the Internet) to a different part of the Internet which is still accessible.⁹⁸ Finally, these regulations may hamper the economic development of many countries, especially China. For example, without substantial foreign investment in the development of China's Internet, China considerably lags behind several of the world's major economic players. They are lacking the ability to utilize the Internet for educational and business applications.⁹⁹ While the Chinese government is encouraging investment in its information infrastructure, China will nonetheless continue to lag behind

⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ *Id.* at 378-9.

⁹⁷ *See* THE HOUSE POLICY COMMITTEE, *supra* note 1.

⁹⁸ Feir, *supra* note 50, at 379.

⁹⁹ *Supra* note 6, at 641.

as long as its strict control of Internet content hampers investment.¹⁰⁰ For the foregoing reasons, it seems highly probable that the proposed legislation will not only pass, but it will be very successful in attaining its goals in regards to international Internet blocking.

THE ROLE OF TECHNOLOGY THAT COUNTERS INTERNET BLOCKING WITHIN THE U.S.

In the midst of focusing on how this legislation would be effective on the international playing field, Congressional leaders have neglected to consider any negative repercussions this legislation may bear on the U.S. home front. Essentially, there has been an unintended clash between U.S. efforts to protect children from inappropriate material and attempts to thwart foreign governments from blocking citizen Web access.¹⁰¹

To combat the influx of sexual expression into homes, various Internet companies have developed systems to help parents' control such material.¹⁰² The World Wide Web Consortium's Platform For Internet Content Selection (PICS) developed technical standards which help parents filter and screen material their children see on the Web.¹⁰³ Also, some companies have developed software, such as Cyber Patrol and Surf Watch, intended to help parents limit Internet access within their homes.¹⁰⁴ However, software

¹⁰⁰ *Id.*

¹⁰¹ THE HOUSE POLICY COMMITTEES *supra* note 1, at 2.

¹⁰² *ACLU v. Reno*, 929 F. Supp. 824, 838 (E.D. Pa. 1996); *Shea v. Reno*, 930 F. Supp. 916, 932 (S.D.N.Y. 1996).

¹⁰³ *ACLU*, 929 F. Supp. at 838; *Shea*, 930 F. Supp. at 932.

¹⁰⁴ *ACLU*, 929 F. Supp. at 839.

that counters Internet blocking and censorship devices, such as the software to be used overseas, can be used by children within the United States. For example, federal law in the United States requires schools to filter content or lose federal funding, but some of the anti-censorship technology could help children get around the blocking.¹⁰⁵ Thus, many legislators may be influenced by a concerned constituency, and limit the amount of funding the bill has planned to allocate in order to delay swift development of the software, or even repudiate the presence of such software on U.S. soil. The impetus for such an action is to stamp out any tool or instrument that thwarts the efforts to protect children from obscene material and preserve the moral integrity of essential aspects of society: America's youth, and the existing substance on the Internet.

However, U.S. courts have previously denied the weight of such an argument pursuant to the protections afforded by the First Amendment.¹⁰⁶ Such technology is considered speech and a form of expression,¹⁰⁷ protected by the First Amendment of the U.S. Constitution. Hence, the possibility of rejecting the use of such software within the U.S. looks bleak, and can be easily dissuaded not only by protecting the software pursuant to the First Amendment, but also protecting the Internet and its users.¹⁰⁸

¹⁰⁵ *Id.*

¹⁰⁶ *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000).

¹⁰⁷ *Id.* at 485.

¹⁰⁸ *Reno v. ACLU*, 521 U.S. 844 (1997).

THE FALL OF THE COMMUNICATIONS DECENCY ACT

Concern over children's access to obscene and indecent material via the Internet led Congress to pass the Communications Decency Act in 1996.¹⁰⁹ The Act authorizes criminal penalties for anyone who in interstate or foreign communications knowingly uses an interactive computer service to send information, both sexually explicit and otherwise, to persons under eighteen years of age.¹¹⁰ Proponents of the CDA argue that parents alone cannot protect their children from indecent material on the Internet.¹¹¹ During a Senate session, Senator James Exon stated "[o]ne of the things this Senator feels we should properly address...is the matter of trying to clean up the Internet--to make that superhighway a safe place for our children and our families to travel on...It is not an exaggeration to say that the worst, most vile, most perverse pornography is only a few click-click-clicks away from any child on the Internet. . . The fundamental purpose of the [CDA] is to provide much-needed protection for [our] children."¹¹² However, these provisions were immediately challenged by numerous citizens' groups and electronic publishers. The issue was brought before the Supreme Court in 1997 in the landmark case Janet Reno v. American Civil Liberties Union. Justice Stevens delivered the opinion of the Court, stating that the CDA lacked the precision that the First Amendment requires when a statute regulates the content of speech: Any regulation of speech that is content-based raises special First Amendment concerns because of its obvious chilling effect on

¹⁰⁹ CARTER, ET AL *The First Amendment and the Fourth Estate*, 959 (Foundation Press 2001).

¹¹⁰ *Id.* at 960.

¹¹¹ Appellant's Brief at ?, *Reno v. ACLU*, 929 F.Supp. 824 (E.D. Pa. 1996) (No. 96-511).

¹¹² 141 CONG. REC. S8087-04 (daily ed. June 5, 1995) (statement of Sen. Exon).

free speech.¹¹³ The Court went on to say that the deterrent effect the Act intends to instill “poses greater First Amendment concerns than those implicated by other regulations:¹¹⁴ “In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another.”¹¹⁵ Finally, the Court held that the CDA was unconstitutional, stating: “[G]overnmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.”¹¹⁶ The Supreme Court firmly adheres to the idea that governmental control stifles the creativity and freedom of people’s talents that may inevitably be displayed on the Internet, which is contrary to the fundamental essence of democracy, liberty, and freedom.¹¹⁷ Not only is this idea vibrant domestically, but as we can see from the aforementioned legislation, it is also applicable in the international realm.

The *Reno v. ACLU* case set the foundation for finding technological software (such as encryption) an expressive means of communication and therefore protected under the First Amendment. Encryption is now viewed as essential to the security of international electronic commerce, and such software is also directly correlated with

¹¹³ See *Terminiello v. Chicago*, 337 U.S. 1 (1949).

¹¹⁴ See *Denver Area Educational Telecomm. Consortium, Inc. v. Federal Communications Commission*, 116 S. Ct. 2347 (1996).

¹¹⁵ *Supra* note 108, at 855.

¹¹⁶ *Id.* at 860.

¹¹⁷ See Lawrence Lessig, *The Future of Ideas* (Random House 2001).

technology that counters Internet jamming.¹¹⁸ In Junger v. Daley, the U.S. Court of Appeals for the Sixth Circuit held that computer source code (i.e. encryption software, Peek-a-Booty, DynaWeb, and Triangle Boy networks, etc.) is an expressive means for the exchange of information and ideas about computer programming; therefore it is protected by the First Amendment.¹¹⁹ The Court of Appeals looked to the Supreme Court rationale of the *O'Brien* case, which stated that “all ideas having even the slightest redeeming social importance, including those concerning the advancement of truth, morality, the arts, and science have the full protection of the First Amendment (emphasis added).¹²⁰ Thus, because such technological software is considered to be speech and a form of expression, it is protected by the First Amendment of the U.S. Constitution, and it cannot be banned from use in the United States. Not only are there constitutional arguments involved to protect this software, but the economic interests of the U.S. will be greatly served as well. The presence of such products in the computer software market can have a positive effect for the economy as a whole.

CONCLUSION

There are authoritarian governments that consider material on the Internet as being subversive, and as a result, they aggressively block and censor their citizens’ access to it. These efforts can be seen as restricting an individual’s freedom to receive and exchange information, which, under democratic countries’ standards pursuant to the Universal Declaration of Human Rights, is considered to be an implicit right for every

¹¹⁸ *About the Peek-A-Booty Project*, *supra* note 73, at 1005.

¹¹⁹ *Junger*, 209 F.3d at 485.

¹²⁰ *Id.*; see *United States v. O'Brien*, 391 U.S. 367 (1968).

person. Additionally, such Internet restrictions can also impair potential economic gains for every country involved (including the authoritative countries) in international investment that uses the Internet as a moderating tool. In response to this predicament, the United States took the forefront of this defiance by proposing to pass a bill that would counter Internet jamming by utilizing encryption and networked software. However, there are two dilemmas that are delaying its passage: limited support for this bill in regards to it intervening with foreign state sovereignty, and the presence of the encryption software within the United States.

The two primary policies of the legislation is to develop and implement a global strategy to combat state-directed Internet jamming, and to establish the Office of Global Internet Freedom, which will develop and implement technologies to defeat Internet jamming and censorship. The legitimacy of this legislation is found in both economic and political impetuses. The economic reasons to push for the bill's passage are that: numerous U.S. companies are vulnerable to government sanctions, U.S. computer service providers are delaying entry into China due to the uncertainty created by the regulations, U.S. businesses operating or providing Internet service in China must be willing to deal with unpublished rules, governmental censorship and control will slow the development of global Internet access, and the censorship of the Internet may create political tensions with other nations, thus hindering foreign investment. The political rationale to discover the legitimacy of the bill is found in the fact that the authoritative regulations violate the spirit of Article 19 of the Universal Declaration of Human Rights. These reasons account for the likely acceptance of the bill in the global sector.

As for the presence of the bill in the U.S. domestic sector, it has created a clash between U.S. efforts to protect children from inappropriate material and attempts to thwart foreign governments from blocking citizen Web access. As a result, the bill may be delayed in its passage, or the software itself may be banned from use within the U.S. However, such technology is considered speech and a form of expression as stated by the Supreme Court and the U.S. Court of Appeals in the Sixth Circuit. Reno v. ACLU found that the Telecommunications Decency Act of 1996 unconstitutional because it suppressed a larger amount of speech than it intended. And Junger v. Daley, the Court of Appeals held that encryption software is an expressive means for the exchange of information, and is thus protected under the First Amendment. Hence, it is very likely that any domestic opposition to the bill in regards to the fear that it may interfere with the responsibility of protecting children from obscene material on the Internet may be quashed pursuant to the First Amendment.

Consequently, the legislation has the intent to limit both foreign and domestic governmental involvement in the sphere of political and economic information exchange and information gathering based on the premise forwarded by Lawrence Lessig: governmental control stifles the creativity and freedom of people's talents that may inevitably be displayed on the Internet, which is contrary to the fundamental essence of democracy, liberty, and freedom.