DePaul Journal of Art, Technology & Intellectual Property Law

Volume 13
Issue 1 *Spring 2003*

Article 9

Global Internet Freedom: Can Censorship and Freedom Coexist?

Elaine M. Chen

LEGISLATIVE UPDATE

GLOBAL INTERNET FREEDOM: CAN CENSORSHIP AND FREEDOM COEXIST?

I. INTRODUCTION

Christopher Cox (R-CA), House Policy Chairman, and Tom Lantos (D-CA), House International Relations Committee Ranking Member, introduced a new bill on January 7, 2003, to "develop and deploy technologies" to defeat Internet jamming and censorship around the world, entitled the "Global Internet Freedom Act" ("Act").[1] Senators Ron Wyden (D-OR) and Jon Kyl (R-AZ) introduced a nearly identical version in the Senate on October 10, 2002.[2] The Act seeks to establish the Office of Global Internet Freedom in the National Telecommunications and Information Administration, which will develop and implement a comprehensive global strategy to combat state-sponsored and state-directed Internet censorship and persecution of those who use censored Internet sites.[3] The Act expresses the Congressional

1. H.R. 48, 108th Cong. (1st Sess. 2003), *available at* http://thomas.loc.gov.

2. S. 3093, 107th Cong. (2d Sess. 2002), *available at* http://thomas.loc.gov.

3. H.R. 48 § (2). The Congress makes the following findings: (1) Freedom of speech, freedom of the press, and freedom of association are fundamental characteristics of a free society. The first amendment to the Constitution of the United States guarantees that 'Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble.' These constitutional provisions guarantee the rights of Americans to communicate and associate with one another without restriction, including unfettered communication and association via the Internet. Article 19 of the United Nation's Universal Declaration of Human Rights explicitly guarantees the freedom to 'receive and impart information and ideas through any media and regardless of frontiers'. (2) All people have the right to communicate freely with others, and to have unrestricted access to news and information, on the Internet. (3) With nearly 10 percent of the world's population now online, and more gaining access each day, the Internet stands to become the most powerful engine for democratization and the free exchange of ideas ever invented. (4)

Unrestricted access to news and information on the Internet is a check on repressive rule by authoritarian regimes around the world. (5) The governments of Burma, Cuba, Laos, North Korea, the People's Republic of China, Saudi Arabia, Syria, and Vietnam, among others, are taking active measures to keep their citizens from freely accessing the Internet and obtaining international political, religious, and economic news and information. (6) Intergovernmental, nongovernmental, and media organizations have reported the widespread and increasing pattern by authoritarian governments to block, jam, and monitor Internet access and content, using technologies such as firewalls, filters, and 'black boxes'. Such jamming and monitoring of individual activity on the Internet includes surveillance of e-mail messages, message boards, and the use of particular words; 'stealth blocking' individuals from visiting websites; the development of 'black lists' of users that seek to visit these websites; and the denial of access to the Internet. (7) The Voice of America and Radio Free Asia, as well as hundreds of news sources with an internet presence, are routinely being jammed by repressive governments. (8) Since the 1940s, the United States has deployed anti-jamming technologies to make Voice of America and other United States Government sponsored broadcasting available to people in nations with governments that seek to block news and information. (9) The United States Government has thus far commenced only modest steps to fund and deploy technologies to defeat Internet censorship. To date, the Voice of America and Radio Free Asia have committed a total of $1,000,000 for technology to counter Internet jamming by the People's Republic of China. This technology, which has been successful in attracting 100,000 electronic hits per day from the People's Republic of China, has been relied upon by Voice of America and Radio Free Asia to ensure access to their programming by citizens of the People's Republic of China, but United States Government financial support for the technology has lapsed. In most other countries there is no meaningful United States support for Internet freedom. (10) The success of United States policy in support of freedom of speech, press, and association requires new initiatives to defeat totalitarian and authoritarian controls on news and information over the Internet.

H.R. 48 § (3) states: The purposes of this Act are: (1) to adopt an effective and robust global Internet freedom policy; (2) to establish an office within the International Broadcasting Bureau with the sole mission of countering Internet jamming and blocking by repressive regimes; (3) to expedite the development and deployment of technology to protect Internet freedom around the world; (4) to authorize the commitment of a substantial portion of United States international broadcasting resources to the continued development and implementation of technologies to counter the jamming of the Internet; (5) to utilize the expertise of the private sector in the development and implementation of such technologies, so that the many current technologies used commercially

desire for the United States to: (1) denounce governments that restrict, censor, ban, and block access to information on the Internet; (2) direct the U.S. Representative to the United Nations to submit a resolution condemning such actions; and (3) deploy technologies aimed at defeating state-directed Internet censorship and the persecution of those who use the Internet.[4]

Although the Act has won support from bipartisan members of Congress and human rights organizations, the Act will face a difficult time establishing its legitimacy for several reasons. These reasons include, but are not limited to: current domestic regulation and enforcement of the Internet including the Supreme Court's interpretation of the First Amendment as it pertains to the Internet, confrontation with powerful domestic corporations that have business partnerships with foreign countries that censor, and ramifications of current events surrounding the current global image of the United States. Although the focus of this legislation is based on a very legitimate human rights issue with several justifiable positions, it will most likely not pass. The Act includes limitations on its authority to interfere with foreign national censorship that is also in furtherance of legitimate law enforcement aims consistent with the Universal Declaration of Human Rights.[5]

---

for securing business transactions and providing virtual meeting space can be used to promote democracy and freedom; and (6) to bring to bear the pressure of the free world on repressive governments guilty of Internet censorship and the intimidation and persecution of their citizens who use the Internet.

4. H.R. 48 § 5, which states "It is the sense of the Congress that the United States should: (1) publicly, prominently, and consistently denounce governments that restrict, censor, ban, and block access to information on the Internet; (2) direct the United States Representative to the United Nations to submit a resolution at the next annual meeting of the United Nations Human Rights Commission condemning all governments that practice Internet censorship and deny freedom to access and share information; and (3) deploy, at the earliest practicable date, technologies aimed at defeating state-directed Internet censorship and the persecution of those who use the Internet."

5. H.R. 48 § 4(e), which states "Nothing in this Act shall be interpreted to authorize any action by the United States to interefere with foreign national censorship in furtherance of legitimate law enforcement aims that is consistent with the Universal Declaration of Human Rights."

However, by creating a committee that will focus on defeating international censorship, interference with foreign national censorship will become inevitable and eventually create conflict. Internet censorship and jamming protocol should be left to an international arena, such as the United Nations, where a more "neutral" Internet resolution can be enforced.

Part II of this paper will include a background section examining the legislative history that led to the Act, explore the growth of the Internet and its global effects, and examine the goals of this current legislation. This background section will demonstrate the current domestic trend of a global human rights responsibility, especially addressing other medias and their effects. Further, this section will highlight the evolution of the Internet and its historical significance on our global and domestic economy. Part III will address current global Internet regulations, examine The People's Republic of China ("China") – the main offender, and address recent Supreme Court interpretation of the First Amendment. In particular, the analysis section will examine *Reno v. American Civil Liberties Union* ("ACLU"),[6] *Ashcroft v. ACLU,*[7] and *Ashcroft v. Free Speech Coalition.*[8] Finally, in questioning the Act, Part IV will examine the legal enforcement of the Internet focusing on regulation regarding the music industry and the ramifications of Napster Inc. and Internet gambling. Additionally, this section will address the Act's likelihood of passage, weighing both the lobbying power of corporations that supply the hardware and software to foreign countries that censor, and the effects of current events of the war in Iraq and the United States' current global image.

In addition, this essay will consider the role of the Act as having an advisory relationship with the issue of a global Internet and discuss why the ultimate goal of the legislation is crucial in light of current news regarding the outbreak of Severe Acute Respiratory Syndrome ("SARS"). In conclusion, efforts from human rights

6. Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).
7. Ashcroft v. American Civil Liberties Union, 535 U.S. 564 (2002).
8. Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).

groups and the private sector are noteworthy, yet without the overwhelming support in Congress, ingenious computer hackers will have to continue to seek private support to aid those people that live under governmental censorship of the Internet.

II. BACKGROUND

The purpose of this section is to examine the legislative history that led to the Act, to explore the evolution and historical significance of the Internet, and to introduce the goals set out in the Act. This proposed legislation by House Policy Chairman, Christopher Cox (R-CA), focuses on the recognition of the rights of freedom of speech, press, and association as universal and fundamental human rights for all people. It also requires new initiatives to defeat totalitarian controls over the Internet.

The Internet is a revolutionary media, initially created for the U.S. military, that has only been in existence for the last thirty years, moreover, only in the last decade has it made a significant impact on society. Examples of some of the topics that will be examined are how the Internet works and why it has become an important commercial, educational, and social tool.

A. Borderless Fundamental Right: The Evolution of Legislative History and Policy Concerns of Free Speech

Since the 1940's the United States has deployed anti-jamming technologies to make Voice of America ("VOA") and other United States government sponsored broadcasting available to people in nations with governments that seek to block news and information.[9] VOA is an international multimedia broadcasting service funded by the U.S. government[10] that broadcasts more than

9. H.R. 48 § 2(8), which states in relevant part "Since the 1940s, the United States has deployed anti-jamming technologies to make Voice of America and other United States Government sponsored broadcasting available to people in nations with governments that seek to block news and information."

10. Fast Facts on Voice of America, *available at* http://www.voa.gov/index.cfm?sectionTitle=Fast%20Facts (last visited April 9,

1,000 hours of news, informational, educational, and cultural programs every week to an audience of some 94 million people worldwide.[11] It also has an active website that publishes and broadcasts its program live in other languages including Arabic, Chinese, Russian, Albanian, Spanish, and Persian.[12]

VOA began in response to the perceived need of people in closed and war-torn societies for a consistently reliable and authoritative source of news. In 1939, the American playwright Robert Sherwood, who would become a speechwriter for President Franklin Roosevelt and later, the "father of the Voice of America,"[13] predicted the impact of international broadcasting when he said: "We are living in an age when communication has achieved fabulous importance. There is a new decisive force in the human race, more powerful than all the tyrants. It is the force of massed thought-thought which has been provoked by words, strongly spoken."[14] In 1941, President Roosevelt established the U.S. Foreign Information Service ("FIS") and named speechwriter Sherwood as its first director.[15] Driven by his belief in the power of ideas and the need to communicate America's views abroad, Sherwood established his headquarters in New York City, recruited a staff of journalists, and began producing material for broadcast to Europe by the privately-owned American shortwave stations.[16]

With Japan's attack on Pearl Harbor and Germany's declaration of war against the United States, FIS made its first direct broadcasts to Asia from a studio in San Francisco.[17] Subsequently, FIS beamed its first broadcast to Europe just 79 days after the

---

2003).

11. *Id.*

12. Voices of America – Internet, *available at* http://www.voa.gov/index.cfm?sectionTitle=Internet (last visited April 9, 2003).

13. *Id.*

14. The Beginning: An American Voice Greets the World, *available at* http://www.voa.gov/index.cfm?tableName=tblVOAHistory&articleID=10016&sectiontitle=VOA%20History (last visited April 9, 2003).

15. *Id.*

16. *Id.*

17. *Id.*

United States entered World War II.[18] Announcer William Harlan Hale opened the German-language program with the words: "Here speaks a voice from America."[19] From the beginning, VOA promised to tell its listeners the truth, regardless of whether the news was good or bad.[20]

Currently, VOA still exists and is funded by the United States government and located in Washington D.C. For fiscal year 2002, the U.S. Congress appropriated $147 million for VOA, including funds for radio and television, exclusive of transmission and other support activities.[21] These supported activities include projects targeted at stopping repressive governments from jamming the transmission of news provided by VOA, Radio Free Asia ("RFA"), [22] as well as hundreds of other news sources that can transmit their information to people living in countries ruled by repressive governments.

B. Historical Overview of the Internet and Its Effects on Society

The Internet is an international network of interconnected computers. With the decline in the cost of hardware over the past three decades the Internet has been in existence, it has become more accessible to people around the world. The Internet is the outgrowth of what began in 1969 as a military program called "ARPANET," which was designed to enable computers operated by the military, defense contractors, and universities conducting defense-related research, to communicate with one another

18. *Id.*

19. *Id.*

20. *See supra*, note 14.

21. *See* Fast Facts on Voice of America, *supra* note 10.

22. About RFA, *available at* http://www.rfa.org/front/about/ (last visited April 9, 2003). Radio Free Asia came into being on March 1996 as a private corporation with funding voted by the U.S. Congress and then funneled to RFA by the Broadcasting Board of Governors, which oversees all U.S. international broadcasters. The job of RFA is to bring news and information about their own country to populations denied the benefits of freedom of information by their governments. For additional discussion on the access to information in Asia, specifically China, *see infra* Part III § B.

through redundant channels. The redundancy of this system guaranteed reliable communications capabilities even if some portions of the network were damaged in a war. While the ARPANET no longer exists, it provided the basis for the development of a number of civilian computer networks that would eventually link with each other to form what we now generically refer to as the "Internet." This has ultimately enabled millions of people to communicate with one another and access vast amounts of information from around the world.[23]

Today, nearly 10 percent of the world's population is online and 4-in-5 households in the United States with computers had at least one member using the Internet.[24] In the United States according to the Commerce Department's Census Bureau, 54 million households, or 51 percent, had one or more computers in the home in August 2000, up from 42 percent in December1998.[25] People

---

23. *See* Reno, *supra* note 6, at 849.

24. The House Policy Committee, Policy Statement, Tear Down This Firewall, *available at* http://policy.house.gov/html (last visited March 20, 2003).

25. Eric Newburger, 9-in-10 School-Age Children Have Computer Access; Internet Use Pervasive, Census Bureau Reports, September 6, 2001, *available at* http://www.census.gov/Press-Release/www/2001/cb01-147.html (last visited April 9, 2003). The full text of the report is as follows: A ratio of 9-in-10 school-age children (6-to-17 years old) had access to a computer in 2000, with 4-in-5 using a computer at school and 2-in-3 with one at home, according to a report released today by the Commerce Department's Census Bureau. The report showed that 54 million households, or 51 percent, had one or more computers in the home in August 2000, up from 42 percent in December 1998.
"Since 1984, the country has experienced more than a five-fold increase in the proportion of households with computers," said Census Bureau analyst Eric Newburger, author of Home Computers and Internet Use in the United States: August 2000. "In addition, Internet use is rapidly becoming synonymous with computer availability."
In 2000, more than 4-in-5 households with computers had at least one member using the Internet at home (44 million households). When the Census Bureau first collected data on Internet use in 1997, fewer than half of the households with computers had someone who was able to go online.
The report measured the influence of the Internet on how people access and use information. Of the total U.S. population, about 1-in-3 adults used e-mail from home in 2000, and nearly 1-in-4 used the Internet to
search for information about topics such as business, health or government

not only receive global news over the Internet, rather, the Internet is also used to pay bills, chat to friends, send messages known as e-mail, conduct business, and for other various daily activities. It has revolutionized how we communicate and how business is conducted. The Internet has also become a powerful tool for democratization and a forum for the free exchange of ideas. In

---

services. Nearly 1-in-5 used the Internet to check on news, weather or sports. And 1-in-8 adults performed job-related tasks using a home
Internet connection.
Other highlights:
- Nearly 9-in-10 family households with annual incomes of $75,000 or more had at least one computer and about 8-in-10 had at least one household member who used the Internet at home.
- Among family households with incomes below $25,000, nearly 3-in-10 had a computer and about 2-in-10 had Internet access.
- Two-thirds of households with a school-age child had a computer, and 53 percent had Internet access.
- E-mail is the most common Internet application at home, used by 88 percent of adults and 73 percent of children who are online.
- Single-person households were the least likely to have a computer (30 percent) or Internet access (24 percent). In households with two to four persons, 58 percent had a computer and 47 percent had Internet access.
- Households in the West were the most likely to have computers (57 percent) and Internet access (47 percent). Those in the South were the least likely to have computers (47 percent) and Internet connections (38 percent).
- Ninety-four million people used the Internet at home in 2000, up from 57 million in 1998.
- Nearly two-thirds (65 percent) of all children 3-to-17 years old lived in a household with a computer in 2000, up from 55 percent in 1998. About 3-in-10 children used the Internet at home, compared with about 2-in-10 in 1998.
- Schools have "leveled the playing field" by giving computer access to children who do not have one at home. Computer use at school was more nearly equal across various income, race or ethnic groups than was access at home.
- About 77 percent of White non-Hispanic and 72 percent of Asian and Pacific Islander children lived in households with computers, while only 43 percent of African American children and 37 percent of Hispanic children did.
The report uses Current Population Survey (CPS) data obtained from about 50,000 U.S. households. The data should not be confused with results from Census 2000, which did not include questions on computer access and Internet use. Statistics from sample surveys, such as CPS, are subject to sampling and nonsampling error.

fact, one of the greatest aspects about the Internet is that it is essentially autonomous, that is, nobody "owns" it. It is a global collection of networks that connect together in many different ways to form the single entity that is known as the Internet.[26]

Every computer that is connected to the Internet is part of a network. For example, a modem will dial a local number to connect to an Internet Service Provider ("ISP").[27] At work, a local area network ("LAN") may be used, but companies also still connect to the Internet using an ISP with an Internet provider that it has contracted with.[28] Subsequently, the ISP may then connect to a larger network and become part of that network, creating the "Internet".[29] Thus, the Internet is simply a network of networks.

Many countries, especially those of repressive governments, monitor individual activity through the Internet. While some countries randomly read private e-mails, other countries have massive firewalls to prevent the accessibility of censored information.[30] These countries also have monopolies over ISPs that restrict people's access to the Internet.[31] A firewall is simply a program or hardware device that filters the information coming through the Internet connection into a private network or computer system. Many large corporations utilize firewalls to regulate its' employees from accessing what the corporation has deemed to be inappropriate information, as well as to protect their LAN from harmful computer viruses. These corporate firewalls, although on a much smaller scale, are very similar to the firewalls that some

26. How Internet Infrastructure Works, *available at* http://www.howstuffworks.com (last visited March 20, 2003). Internet servers make the Internet possible. All of the machines on the Internet are either servers or clients. The machines that provide services to other machines are servers and the machines that are used to connect to those services are clients. There are Web servers, e-mail servers, FTP servers and etc. serving the needs of Internet users all over the world.

27. *Id.*

28. *Id.*

29. *Id.*

30. *See* Tear Down This Firewall, *supra* note 24.

31. *Id.*

countries utilize to restrict their citizen's access to the Internet.[32]

For example, China used a firewall to block access to the Google Internet search engine; diverting users instead to local Chinese search engines.[33] Internet search engines are special sites on the Web that are designed to help people find information stored on other sites.[34] When the site was reopened to users, Chinese surfers found their browsers' cache function disabled. The cache function, which is a portion of every computer's memory, was once an easy way to access information from banned Websites, however, Chinese authorities continue to find methods to keep their citizens away from politically sensitive information on the Internet.[35]

China has created a very effective Internet censorship system and police force with the filtering software and hardware technology of many U.S. companies such as Microsoft, Sun Microsystems, Cisco and Websense.[36] To many Internet freedom

---

32. *See* How Internet Infrastructure Works, *supra* note 26.

33. Murray Hiebert, *Hackers Fight China's Internet Curbs*, THE WALL STREET JOURNAL, Nov. 6, 2002, at B11B.

34. How Internet Search Engines Work, *available at* http://www.howstuffworks.com (last visited March 20, 2003).The good news about the Internet and its most visible component, the World Wide Web, has hundreds of millions of pages available, waiting to present information on an amazing variety of topics. On the other hand, the bad news about the Internet is that there are hundreds of millions of pages available, most of them titled according to the whim of their author, almost all of them sitting on servers with cryptic names. When you need to know about a particular subject, how do you know which pages to read? If you're like most people, you visit an Internet search engine. There are differences in the ways various search engines work, but they all perform three basic tasks: 1) they search the Internet - or select pieces of the Internet - based on important words; 2) they keep an index of the words they find, and where they find them; and 3) they allow users to look for words or combinations of words found in that index.

35. Oxblood Ruffin, *Great Firewall of China*, REED BUSINESS INFORMATION U.K., November 9, 2002, at 27.

36. Paul Mooney, *China's Cyber Crackdown*, NEWSWEEK, December 16, 2002, at 26. In a report issued last month, Amnesty International singled out Microsoft, Sun Microsystems, Cisco and Websense as U.S. corporations that are increasingly selling filtering hardware and software, among other products, to

activists, the actions of these large corporations are intolerable. However, with Western firms competing for a share of China's rapidly expanding technology market it is a safe bet that they will continue to be drawn to morally questionable alliances.[37]

C. The Goals of the Proposed Legislation

The Global Internet Freedom Act is a piece of legislation introduced in both the United States House of Representatives and the Senate. The purpose of this Act is to (1) adopt an effective and robust global Internet freedom policy; (2) to establish an office within the International Broadcasting Bureau with the sole mission of countering Internet jamming and blocking by repressive regimes; (3) to expedite the development and deployment of technology to protect Internet freedom around the world; (4) to authorize the commitment of a substantial portion of United States international broadcasting resources to the continued development and implementation of technologies to counter the jamming of the Internet; (5) to utilize the expertise of the private sector in the development and implementation of such technologies, so that the many current technologies used commercially for securing business transactions and providing virtual meeting space can be used to promote democracy and freedom; and (6) to increase pressure from the free world on repressive governments guilty of Internet censorship and intimidation.[38]

The Act would direct $100 million over two years to the new office named the Office of Global Internet Freedom (hereinafter in this Act referred to as the "Office") that would become part of the

---

Chinese authorities. Eric Gutmann, a visiting fellow at the Project for the New American Century, a conservative Washington D.C., think tank, claims that Chinese engineers familiar with Cisco's operations told him that the U.S. company had "gone out of the way" to adapt its routers and firewall technology for China.

37. *Id.* China's technology market is estimated to be worth more than $20 billion a year.

38. H.R. 48 § 3.

International Broadcasting Bureau, which includes the VOA.[39] A Director would be appointed who shall develop and implement a comprehensive global strategy to combat state-sponsored and state-directed Internet jamming, and persecution of those who use the Internet.[40] Under the bill, the Office's main objective would be to develop and deploy anti-filtering technologies and provide Congress with an annual report regarding countries that censor the Internet.[41]

In a report to Congress on March 1, following the date of enactment and annually thereafter, the Director of the Office would be required to submit to Congress a report that lists the countries that pursue policies of Internet censorship, blocking, and other abuses; provide information concerning the government agencies or quasi-governmental organizations that implement Internet censorship; and describe with particularity and technical means by which such blocking and other abuses are accomplished.[42] In addition, this report would create a list of

39. *Id.* at § 4(a), (b), which states in whole "(a) ESTABLISHMENT OF OFFICE OF GLOBAL INTERNET FREEDOM- There is established in the International Broadcasting Bureau the Office of Global Internet Freedom (hereinafter in this Act referred to as the 'Office'). The Office shall be headed by a Director who shall develop and implement a comprehensive global strategy to combat state-sponsored and state-directed Internet jamming, and persecution of those who use the Internet. (b) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated to the Office $50,000,000 for each of the fiscal years 2003 and 2004."

40. *Id* at § 4(a).

41. *Id.* at § 4(d), which states in whole "(d) REPORT TO CONGRESS- On March 1 following the date of the enactment of this Act and annually thereafter, the Director of the Office shall submit to the Congress a report on the status of state interference with Internet use and of efforts by the United States to counter such interference. Each report shall list the countries that pursue policies of Internet censorship, blocking, and other abuses; provide information concerning the government agencies or quasi-governmental organizations that implement Internet censorship; and describe with the greatest particularity practicable the technological means by which such blocking and other abuses are accomplished. In the discretion of the Director, such report may be submitted in both a classified and nonclassified version."

42. *Id.*

companies that sell the hardware and software to countries that censor the Internet. There does not appear to be any legal ramifications for those on the list, but groups supporting the Act hope publicity, or possibly placing sanctions on them, would deter these companies from further sales.

The Office would also work with the private sector, which consists of a loose collection of Chinese dissidents and computer hackers (also known as "hacktivists"), to test the ingenuity of foreign censors.[43] According to the Policy Statement by The House Policy Committee, this group of for-profit corporations and non-governmental organizations, are developing and employing various techniques and technologies such as proxy servers, intermediaries, "mirrors," and encryption to overcome state efforts to deny freedom of the Internet.[44] Currently, the U.S., through Voice of America and Radio Free Asia, have budgeted a total of $1 million for technology to counter China's Internet jamming by using technology including "Triangle Boy," produced by SafeWeb.[45] This technology has been successful, but due to the high costs, the service was discontinued. At the time it was discontinued it was reported that it had received millions of hits per month from China and Saudi Arabia.[46] Yet VOA and RFA must rely upon such technologies to ensure access to their programming. Other technologies and products, including Peek-a-Booty, DynaWeb, and Freenet-China, are also currently in use to help keep information flowing in and out of areas where Internet censorship and jamming are prevalent.[47]

These hackers are mostly privately run groups that all have one thing in common - they all desire global Internet freedom. Triangle Boy was a pilot project that allows users to access the World Wide Web through an encrypted channel. SafeWeb Inc. received funding from the U.S. Central Intelligence Agency venture-capital fund to develop the software and was paid by the

43. *See* Mooney, *supra* note 36.
44. *See* Tear Down This Firewall, *supra* note 24.
45. *Id.*
46. *Id.*
47. *Id.*

Voice of America to help Chinese listeners access the radio station's blocked Website.[48] Canadian programmer Paul Baranowski, who works out of his Toronto apartment, funds Peekabooty.[49] Baranowksi, who works on the program, explains that when people on the Internet using his software confront a blocked Internet site, they inform a network of computers running Peekabooty that then finds the requested information and returns it to the original computer in encrypted form.[50] In addition, Dybaweb was launched in North Carolina by a group of Chinese-American engineers keen to open the Internet to users in China. Dynaweb is designed to help Chinese users access blocked Internet sites and download banned documents. Currently, it is difficult for China to attack this system because it regularly changes its numerical Internet portal address, which the government's firewalls use to identify sites.[51] However, it is also very expensive and time consuming to continuously change numerical Internet portal addresses. Finally, Freenet-China is an anonymous P2P (peer-to-peer)[52] network from which users can download without fear of the China Net police.[53] There are many other private sector "hacktivists" and more every day working to introduce new technology and loop holes in the censors of repressive governments.

The Office would direct some of the funds from the Act to these

48. *See* Hiebert, *supra* note 33.

49. *See* Mooney, *supra* note 36.

50. *See* Hiebert, *supra* note 33.

51. *Id.*

52. Peer-to-Peer technology is similar to what was used by Napster Inc. Napster is a different way to distribute MP3 files. Instead of storing the songs or data on a central computer, the data lives on users' machines. This is called peer-to-peer sharing, or P2P. When you want to download a song using programs like Napster, you are downloading it from another person's machine, and that person could be your next-door neighbor or someone halfway around the world.

53. China Steps Up Net Censorship, *available at* http://www.p2pnet.net/issue02/page1.html (last visited April 9, 2003). For a more thorough examination of censorship and its enforcement in China, *see infra* Part III § B.

private sector hackers who have claimed they would use the money provided by Mr. Cox's legislation to "expand our server, make our performance better and respond to any technology China develops to stop us."[54] According to Baronowski, "the final victory will belong to the side willing to invest the most."[55]

Thus, it can be concluded from this background section that, the use of the Internet has created an extreme conflict between governments that censor and governments that consider speech a global fundamental right. The Internet has essentially become a Pandora's Box for many repressive countries, potentially harming their government system. The proposed legislation that is the subject of this essay attempts to review American Internet jurisprudence in the following section to further explore this issue.

III. ANALYSIS

The purpose of this section is to provide a comprehensive analysis of current Internet worldwide regulation, its main offender, China, and American Internet jurisprudence. Although the focus of most Internet censorship literature is on China's policies, many other countries around the world also censor the access of the Internet to its citizens. Nevertheless, the predominant offender is China, which has the largest population accessing the Internet. On the topic of Chinese Internet technology, Greg Walton, a free-lance researcher focusing on the impact of technology on human rights wrote:

> China's security apparatus announced an ambitious plan: to build a nationwide digital surveillance network, linking national, regional and local security agencies with a panoptic web of surveillance. Beijing envisions the Golden Shield as a database-driven remote surveillance system – offering immediate access to records on every

54. *See* Hiebert, *supra* note 33.

55. *See* Mooney, *supra* note 36.

citizen in China, while linking to vast networks of cameras designed to increase police efficiency.[56]

---

56. Greg Walton, China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China, *available at* http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html#N1 (last visited April 9, 2003). The following is an excerpt from the text: At a trade show held in Beijing in November 2000, the biggest names in Web technology – "companies that proudly attach themselves overseas to the Internet's reputation for anarchy" – peddled their wares to China's secret police and security officials. Billed as the "largest national security exhibition," Security China 2000 was the second such event sponsored by the Ministry of Public Security (MPS) in as many years. Among the organizers listed was the "Chinese Communist Party Central Committee's Commission for the Comprehensive Management of Social Security," a body which is in overall charge of the state security apparatus, from controls over migrant workers, to anti-crime campaigns and monitoring dissident activity.

Shanghai Business Magazine recently estimated that the Chinese security industry is enjoying 15% annual growth. Overseas specialists cited in the trade journal Security World predict 20% growth for the next three to five years. China is expected to become the second largest security market after the US within 10 years.

The trade show was organized by Hong Kong-based Adsale Exhibition Services Ltd. and drew approximately 300 companies from over 16 countries, as well as 24,500 visitors from over 26 of China's provinces. Special guests included Jia Chunwang, Minister of Public Security. According to Adsale, in comparison to the first Security China exhibit in 1998, in 2000 "the show boasts a 50% increase in international exhibitors and an 80% growth in exhibit space area." Exhibitors included network giants Siemens, Motorola, Cisco Systems, Sun Microsystems, and Nortel Networks. There were participating companies from the US, Israel, France, Germany, the Netherlands, Japan, and Canada, among others. The United Kingdom, world leader in closed-circuit TV, had a special section in the show.

China's Golden Shield

The focus of Security China 2000 quickly became the MPS' new Golden Shield project, launched to promote "the adoption of advanced information and communication technology to strengthen central police control, responsiveness, and crime combating capacity, so as to improve the efficiency and effectiveness of police work." China's security apparatus announced an ambitious plan: to build a nationwide digital surveillance network, linking national, regional and local security agencies with a panoptic web of surveillance. Beijing envisions the Golden Shield as a database-driven remote surveillance system – offering immediate access to registration records on every citizen in China, while linking

It is clearly apparent that China has invested a great deal of effort and money to censor information on the Internet. In addition, this section will examine recent United States Supreme Court rulings regarding Internet regulation and censorship. The cases *Reno v. American Civil Liberties Union ("ACLU"),*[57] *Ashcroft v. ACLU,* [58] and most recently *Ashcroft v. Free Speech Coalition*[59] will demonstrate the Courts current conflict with balancing the First Amendment with social concerns of excessive and indecent information over the Internet.

A. Current Internet Regulation Worldwide

Many countries with mostly non-democratic regimes currently restrict access to the Internet. Cuba, Laos, Burma, Saudi Arabia, Syria, Tunisia, Vietnam, Yemen and China are the most notorious violators of Internet freedom.[60] These governments, according to the U.S. State Department and such organizations as Human Rights Watch[61] and Reporters Without Borders,[62] are using

---

to vast networks of cameras designed to cut police reaction time to demonstrations.

Though the project is still in its infancy, Chinese industry executives at the trade fair estimated that the government had spent RMB 600 million (US$70 million) on research to date, and that the total spending would likely run many times that.

The Golden Shield project, according to information on the conference Web site, is focused on the following fields of security: "Access Control, Anti-Hacker Intrusion, Communication Security, Computer Accessories & Software, Decryption & Encryption, E-commerce Security, Extranet & Intranet Security, Firewalls, Networking Communications, Network Security & Management, Operation Safety, Smartcard Security, System Security, Virus Detection, IT-related Services and Others."

57. *See* Reno, *supra* note 6.

58. *See* Ashcroft, *supra* note 7.

59. *See* Free Speech Coalition, *supra* note 8.

60. *See* Tear Down This Firewall, *supra* note 24.

61. Human Rights Watch http://www.hrw.org/ is the largest human rights organization based in the United States. Human Rights Watch researchers conduct fact-finding investigations into human rights abuses in all regions of the world. Human Rights Watch then publishes those findings in dozens of books

methods of control that include denying their citizens access to the Internet, censoring content, banning private ownership of computers, and even making e-mail accounts so expensive that ordinary people cannot use them.[63]

In Cuba all computers are registered with the government, whose intelligence services monitor their e-mail.[64] Citizens in Laos are denied access to sites in other countries that may include sources of "subversive information." Laotians are required to also provide their e-mail passwords to the government so they may intercept and read all e-mails.[65] Similarly, in Burma, Reporters Without Borders reports that Internet use is available to a select few. This limited Internet access is available only through the country's one ISP, which is owned and operated by the Ministry of Defense.[66] It is reported that Burmese dissidents that are active on the web receive virus-infected messages from this government organization.[67]

---

and reports every year, generating extensive coverage in local and international media. This publicity helps to embarrass abusive governments in the eyes of their citizens and the world. Human Rights Watch then meets with government officials to urge changes in policy and practice - at the United Nations, the European Union, in Washington and in capitals around the world.

62. Reporters Without Borders Website http://www.rsf.org, Reporters Without Borders is kept on constant alert via its network of over 100 correspondents, rigorously condemns any attack on press freedom world-wide by keeping the media and public opinion informed through press releases and public-awareness campaigns. The association defends journalists and other media contributors and professionals who have been imprisoned or persecuted for doing their work. It speaks out against the abusive treatment and torture that is still common practice in many countries. The organization supports journalists who are being threatened in their own countries and provides financial and other types of support to their needy families. Reporters Without Borders is fighting to reduce the use of censorship and to oppose laws designed to restrict press freedom.

63. *See* Tear Down This Firewall, *supra* note 24.

64. *Id.* Messages from outside the country are received hours after being sent, or not at all.

65. *Id.*

66. *Id.*

67. *Id.* All e-mails are screened by Myanmar Post and Telecommunications

The Syrian government can filter every e-mail account in the country because it controls the only Internet service provider; Saudi authorities appear to filter all public Web requests and e-mail traffic as well.[68] In Syria, the government's Telecommunications Establishment, blocks access to "offensive" content and all pro-Israeli sites. In order for Syrians to connect to the Internet, a government technician must come to their home, install the software, and assign the user's password.[69]

All five Internet services in Tunisia are under the control of the government and the Tunisian Internet Agency, created in 1996, which regularly provides the names of subscribers to the government.[70] In Vietnam, in August 2001, the Prime Minister issued a decree prohibiting use of the Internet "for the purpose of hostile actions against the country or the destabilize security, violate morality, or violate other laws and regulations."[71] Although the Internet is nominally available to anyone who wants to use it, the extremely high prices restrict its usage.[72] Finally, in Yemen, Internet access is severely limited by prohibitive high prices of equipment and Internet subscriptions.[73]

("MPT"), Burma's national telecom operator. In January 2000, MPT banned all political texts and shared Internet accounts. Later in 2000, the Ministry of Communications barred all foreigners from using private e-mails, and required authorization before web pages can be created or modems and fax machines brought into Burma. Violations of these laws regarding Internet usage can result in up to 15 years in prison.

68. *See* Ruffin, *supra* note 35.

69. *See* Tear Down This Firewall, *supra* note 24. In December 2000, for example, the Syrian government detained an individual without charge for forwarding a political cartoon via e-mail.

70. *Id.* Websites and on-line publications in Tunisia that contain information critical of the government are frequently blocked, according to the State Department. Among the websites blacklisted by the Tunisian government is a report on the Internet use in Tunisia by Human Rights Watch.

71. *Id.*

72. *Id.* The government is seeking additional authority to monitor Internet cafes and hold the owners of these cafes responsible for customer use of the Internet. This legislation would affect all of the nearly 4,000 Internet cafes in Vietnam.

73. *Id.* Although officials say the Yemeni government does not block

Countries, such as those described above, are the targets of the Act.[74] This regulation of information may seem oppressive to a Western audience, thereby justifying the goals of the Act. However, a crucial question emerges over whether the U.S. government has such a right to challenge these forms of international policy.

B. China's Golden Shield – the Main Offender

According to one source, there are over 33.7 million Internet users in the People's Republic of China ("China"),[75] but authorities legally restrict and penalize access to any information on the Internet considered "subversive" or "critical" of the state.[76] In recent years, China's legislature enacted several laws and regulations on the use of computers and the Internet, which recognize some personal rights, especially that of an individual's "privacy" in the Internet and the freedom of communications.[77] On the other hand, virtually all of the regulations authorize monitoring, surveillance and control of prohibited content, information and messages by State authorities.[78]

At an Internet trade show in 2002, China introduced their ambitious plan to control the Internet. The Ministry of Public Security's ("MPS") new Golden Shield project, launched to promote "the adoption of advanced information and communication technology to strengthen central police control,

---

political sites, mowj.com, the Yemeni national Opposition Front's website, was blocked by the government, and has now ceased operation completely.

74. H.R. 48 §2(5), which states "The governments of Burma, Cuba, Laos, North Korea, the People's Republic of China, Saudi Arabia, Syria, and Vietnam, among others, are taking active measures to keep their citizens from freely accessing the Internet and obtaining international political, religious, and economic news and information."

75. *See* Tear Down This Firewall, *supra* note 24. Over 250,000 Chinese websites and 200,000 Internet cafes.

76. *Id.*

77. Song Huang & Ruchun Ji, *Privacy Protection in China's Cyberspace*, CHINA LAW & PRACTICE, February 1, 2003, at 29.

78. *Id.*

responsiveness, and crime combating capacity, so as to improve the efficiency and effectiveness of police work."[79] In addition, the MPS also concluded that:

[T]he success of the Golden Shield project depends on a wide range of advanced technologies. While Chinese research is advancing rapidly in these areas, and other related fields, Chinese scientists have developed none of the components necessary to implement Golden Shield independently. In each case, they have relied on assistance from Western corporations, either by purchasing components as turnkey solutions, or through technology transfer – either through formal business deals or in exchange for greater market access. The technologies necessary to support an intelligent mass surveillance.[80]

Furthermore, it has been estimated that China's Internet police force numbers are as high as 40,000 people.[81] This powerful police force demonstrated its abilities in September 2002 when it blocked access to the Google search engine for a week.[82] This technically ingenious yet repressive act of censorship shocked the Internet community and initiated reaction such as the present legislation to stop Internet jamming.

The "right to privacy" is not a distinct right specifically found in any existing Chinese laws or regulations.[83] The Chinese legislature has recently enacted several new laws and regulations on the use of computers and the Internet, which recognize some personal rights, especially that of an individual's "privacy" in use of the Internet and the freedom of communications.[84] These laws remain very limiting because they all authorize monitoring, surveillance and control of prohibited content, information and

79. *See* Walton, *supra* note 56.

80. *Id.*

81. *See* Mooney, *supra* note 36.

82. *Id.*

83. *See* Huang, *supra* note 77. The scope of protection of privacy is not expressly defined or readily ascertainable under current Chinese law, despite the fact that the term "privacy" ("yinsi") is frequently reference in different Chinese laws, regulations and judicial interpretation

84. *Id.*

messages by State authorities, as well as additional control through self-censorship on the part of the providers of Internet information services.[85]

According to the Internet Magazine, Amnesty International has condemned the Chinese government for detaining at least 33 people for offenses related to using the Internet.[86] In its report, *State Control of the Internet in China*, Amnesty cited the closure of many Chinese Internet cafes, the blocking of search engines Google and Alta Vista as major concerns.[87] The report also called for the Chinese authorities to release their 'prisoners of conscience' sentenced to jail for simply expressing their views peacefully over the Internet.[88] According to Chinese authorities these individuals are dissidents who have provided 'state secrets' to others over the Internet, which may be sentenced to death.[89]

For example, since June 3rd, 2000, Mr. Huang Qi, a Chinese citizen and creator of the website *www.6-4tianwang.com* has been held in detention without trial.[90] He set up the first Chinese human rights Web site. Over his website, he had allegedly disseminated subversive information about the Tiananmen massacre in June 1989, as well as, published articles by Chinese dissidents.[91]

---

85. *Id.* All of the existing regulations on the use of computers and the Internet prohibit production, duplication, release or dissemination of content that is contrary to the basic principles laid down in the Constitution; endangers state security; discloses state secrets; subverts state power or sabotages the unity of the State; infringes upon the honor and interests of the State; incites ethnic hostility or racial discrimination; disrupts the social order; disseminates obscenity, pornography, gambling; incites violence, murder or terror; instigates others to commit offenses; insults or defames others, or infringes upon the lawful rights and interests of others; and other content prohibited under laws or administrative regulations.

86. *Amnesty condemns Chinese ways: draconian Internet regulation threatens freedom of speech in China*; INTERNET MAGAZINE, March 1, 2002, at 14.

87. *Id.*

88. *Id.*

89. *Id.*

90. Olivier Dupuis, CELEX Database: Parliamentary Questions, 2002 COMMISSION OF THE EUROPEAN COMMUNITIES, August 8, 2001.

91. *See* Mooney, *supra* note 36.

According to Newsweek, as the police stormed into his house to arrest Huang and his wife, he posted a final message: "The road is still long. Thanks to all who make an effort on behalf of democracy in China. They have come. So long."[92] Cries for help from human rights activists such as Huang Qi and other Internet dissidents around the world will continue to motivate private hacktivists regardless of private or governmental monetary support for a very long time.

C. The First Amendment and the Internet

In the United States a great deal of freedom over the Internet exists, however, the U.S. Supreme Court has recently granted writ of certiorari of several cases dealing with censorship over the Internet. These cases are *Reno v. American Civil Liberties Union ("ACLU"),*[93] *Ashcroft v. ACLU,* [94] and most recently, *Ashcroft v. Free Speech Coalition*.[95] In these cases, the issues revolved around sexually explicit material and child pornography on the Internet, and the extent that they should be censored for publication.

The First Amendment of the United States Constitution provides that:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.[96]

In *Reno*, the Court examined the Communications Decency Act of 1996 (CDA) and ruled that it was unconstitutional due to its

92. *Id.*
93. *See* Reno, *supra* note 6.
94. *See* Ashcroft, *supra* note 7.
95. *See* Free Speech Coalition, *supra* note 8.
96. U.S. CONST. Amend. I.

overbreadth.[97] The court concluded that there was a violation of the First Amendment that provides for the freedom of speech, which is essential to their way of life and the corner stone of democracy in the U.S. system. The *Reno* court prioritized First Amendment rights. This prioritization is critical in order to understand why freedom of speech in America is important, to clarify why this Act was introduced, and to explain why libertarians of free speech fight so vigorously for these rights. Several theories exist on why freedom of speech is a fundamental right.[98] These four major theories are to further self-governance, to aid the discovery of truth via the marketplace of ideas, to promote autonomy, and to foster tolerance.[99]

First, in America, freedom of speech is crucial to a democracy and self-governance because open discussions of candidates are essential for voters to make informed decisions. It is through speech that people can influence their government's choices of policies and public officials can be held accountable through criticisms that can pave the way for their replacement.[100] Second, an argument to protect free speech is discovering the truth through the marketplace of ideas. This argument rationalizes that the truth is most likely to emerge from the clash of ideas and ultimately truth will triumph falsehood.[101] This argument might be flawed, but allowing the government to decide what is true, and right, and suppress all else is a much worse alternative.[102]

The third argument for First Amendment rights is advancing autonomy and the human spirit. Justice Thurgood Marshall observed that "[t]he First Amendment serves not only the needs of the polity but also those of the human spirit – a spirit that demands

97. *See* Reno, *supra* note 6.

98. The Supreme Court has held that some liberties are so important that they are deemed to be "fundamental rights" and that generally the government cannot infringe upon them unless strict scrutiny is met.

99. ERWIN CHEMERINSKY, CONSTITUTIONAL PRINCIPLES AND POLICIES 896 (Richard A. Epstein, ed., Second Edition 2002).

100. *Id.*

101. *Id.* at 897.

102. *Id.*

self-expression."[103] Finally, freedom of speech is an intrinsic aspect of the American psych and promotes tolerance, which is the basic value in our society.[104] The claim is that tolerance is a desirable, if not essential, value, and that protecting unpopular or distasteful speech is itself an act of tolerance. Moreover, such tolerance serves as a model that encourages more tolerance throughout society.[105]

These four theories are not mutually exclusive; therefore, all are important in understanding why freedom of speech is protected, in considering what expression should be safeguarded and what can be regulated, and in appraising the Supreme Court's decisions in this area.[106] These theories are embodied in the text of Supreme Court decisions, which has been faced with addressing the Internet as a unique vehicle of communication. The courts must grapple with freedom of speech and the governmental interest to protect people. In recent cases it appears that the Court is cautious of restricting the freedom of speech, yet moving towards what can be acceptable restrictions.

In *Reno,* the United States Supreme Court struck down sections of a statute that attempted to protect minors from indecent and patently offensive material displayed on the Internet. Ultimately, the Court considered the Internet and invalidated key provisions of the Child Decency Act ("CDA") on constitutional grounds.[107] The law made it a federal crime to transmit obscene or indecent material over the Internet in a manner likely to be accessible to a minor.[108] Specifically, §223(a) of the Act prohibited the knowing

103. Procunier v. Martinez, 416 U.S. 396, 427 (1974) (Marshall, J., concurring).

104. *See* Chemerinsky, *supra* note 99, at 900.

105. *Id.*

106. *Id.*

107. *See* Reno, *supra* note 6, at 858.

108. *Id.* The definition of obscenity used by the Court is (a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

transmission of obscene or indecent messages to any recipient less than 18 years of age. A second provision, §223(d), prohibited the knowing sending or displaying of patently offensive messages in a manner that is available to a person less than 18 years of age. The Court examined the extensive availability of sexually explicit material over the Internet and the problems confronting age verification.[109] They defined sexually explicit material on the Internet to include text, pictures, and chat and "extends from the modestly titillating to the hardest-core."[110] They also examined those sites that restrict access to covered material by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number or code.[111]

The Court noted in *Reno* that the issue before it was distinguishable from the Federal Communications Commission ("FCC") regulation of television and radio as seen in *FCC v. Pacifica Foundation*.[112] In *Pacifica,* the FCC prohibited indecent language over the radio during certain times of the day where children might be listening. In contrast, *Reno* found that the CDA applied to all times of the day and compared the CDA's ability to impose criminal penalties on violators, versus the FCC's ability to only sanction in *Pacifica*. [113] Further, *Reno* recognized that the government has a compelling interest in protecting children from exposure to sexual material, but it said that the government cannot restrict speech available to adults so as to safeguard children.[114] The Court stated the CDA's "open-ended prohibitions embrace all nonprofit entities and individuals posting indecent messages or displaying them on their own computers in the presence of minors. The general, undefined terms 'indecent' and 'patently offensive' cover large amounts of nonpornographic material with serious

109. *Id.* at 849.

110. *Id.* at 853.

111. *Id.*

112. Federal Communications Commission v. Pacifica Foundation, 438 U.S. 726 (1978). In this case the Court upheld the ability of the FCC to prohibit and punish indecent language over television and radio.

113. *Id.*

114. *See* Reno, *supra* note 6, at 875.

educational or other value."[115]

Although the Court properly declared those sections of the statute unconstitutional, the Court's analysis leading to its conclusion was partially erroneous.[116] As with all new media, the Court adopted a medium-specific approach in analyzing the new form of communication.[117] However, the Court failed to perceive the vastness of the Internet, and, as a result, misclassified the medium and applied an improper standard of review.[118] In the end, the Supreme Court declared the prohibition of indecent material over the Internet unconstitutional and held that (1) the CDA's vague provisions chilled free speech since speakers could not be certain if their speech was proscribed; (2) the CDA's provision criminalized legitimate protected speech (including sexually explicit indecent speech) as well as unprotected obscene speech, and thus were overinclusive; (3) since the CDA regulated a fundamental freedom, it must be narrowly tailored; (4) time, place, and manner analysis was inapplicable since the CDA regulated the content of speech, not how it was presented; and (5) the CDA was unconstitutional due to its overbreadth.[119]

The next case the Supreme Court considered regarding the Internet and the First Amendment was *Ashcroft v. ACLU.* [120] The

115. *Id.* at 878.

116. Debra M. Keiser, Note, Regulating The Internet: A Critique of Reno v. ACLU, 62 Alb. L. Rev. 769, 769 (1998).

117. *Id.*

118. *Id.* at 769-770

119. *See* Reno, *supra* note 6, at 878.

120. The Supreme Court remanded and vacated the case to the District Court. In *ACLU v. Ashcroft*, U.S. App. LEXIS 4152, (2003). The district court held that COPA, in failing to satisfy strict scrutiny, had no probability of success on the merits, and was not an abuse of discretion. COPA was a content-based restriction on speech. Although it did purport to serve a compelling governmental interest, it was not narrowly tailored, and thus failed strict scrutiny. Further, it stated that plaintiffs would most likely prove at trial that COPA was substantially overbroad. For purpose of this paper, however, the analysis will be confined to the Supreme Court opinion on *Ashcroft.* The focus for this paper is to discuss the Supreme Court interpretation of the First Amendment over the Internet and how the Court has begun to consider some form of restriction over the Internet.

Supreme Court revisited the issue of government regulation of sexually explicit speech over the Internet and considered the constitutionality of the Child Online Protection Act ("COPA"), which sought to protect children from exposure to sexual material on the Internet. The Court ultimately remanded and vacated the case to the lower courts for further review, but it is apparent from the opinion of the case the Court is not as reluctant to restrict the Internet as in the past. It would ultimately consider a new standard, a "contemporary community" standard, as constitutional and ask the lower courts to review the case again.

After the failure of CDA in *Reno*, the President signed and Congress passed COPA, which requires that operators of commercial websites restrict access by children to material which the average person "applying contemporary community standards" would find offensive to the minors' prurient interest.[121] Furthermore, COPA prohibits any person from "knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, making any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors. . ."[122] This provision limited COPA's coverage to materials that are "harmful to minors," whereas the CDA applied to "indecent" and "patently offensive" communications. Further, COPA defines "material that is harmful to minors" using the three-part test for obscenity set forth in *Miller v. California*.[123]

---

121. *See* Ashcroft, *supra* note 7, at 569.

122. 47 U.S.C.S. § 223 (2003).

123. Miller v. California, 413 U.S. 15, 24 (1973). In Miller, the defendant was convicted of distributing unsolicited sexually explicit material in violation of a California statute making distribution of such obscene materials a misdemeanor. The Appellate Department of the Superior Court of California affirmed the judgment without opinion. The defendant appealed. On appeal, the Court redefined obscenity in a new test setting the basic guidelines for the trier of fact to use in determining whether the work qualified as obscene. "The basic guidelines for the trier of fact must be: (a) whether "the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by

Congress had narrowed the range of content restricted material in COPA analogous to the definition of obscenity; therefore, any variance caused by the statute's reliance on community standards was not substantial enough to violate the First Amendment. In addition, this law applied only to commercial websites and it defined the objectionable material in terms of what would be offensive under community standards.[124] Thus, and perhaps most importantly, the Act does not prohibit material so long as the commercial websites take the necessary steps to exclude children. The law required that websites that contain offensive material take action, such as requiring credit cards or age verification services.[125] The Court expressed no view as to whether COPA was overbroad for other reasons, or whether the trial court correctly concluded that the statute likely would not survive strict scrutiny analysis. The government remained enjoined from enforcing COPA absent further action from the lower court.[126]

In a third case, *Ashcroft v. The Free Speech Coalition*, the Court considered whether the government might ban non-obscene child pornography that does not use children in its production.[127] Ultimately, the Court declared this censorship unconstitutional, emphasizing that the government's interest in banning child pornography is in protecting children; if no children are used in the production of the material, the government does not have an adequate interest to justify prohibiting the material.[128]

The Court considered the Child Pornography Prevention Act of

---

the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value."

124. *Id.*

125. 47 U.S.C.S. § 231 (2003). Restriction of access by minors to materials commercially distributed by means of World Wide Web that are harmful to minors.

126. *See* Ashcroft, *supra* note 7. Justice Thomas, Chief Justice Renquist, and Justice Scalia were content that the statute, as written, was not fatally flawed, but still they had concerns that required remand. The six other Justices, in one way or another, saw problems with vagueness and overbreadth.

127. *See* Free Speech Coalition, *supra* note 8.

128. *Id.*

1996 ("CPPA") and whether it abridges the freedom of speech.[129] The CPPA extends the federal prohibition against child pornography to sexually explicit images that appear to depict minors but were produced without using any real children. The statute prohibits, in specific circumstances, possessing or distributing these images, which may be created by using adults who look like minors or by using computer imaging. The new technology, according to Congress, makes it possible to create realistic images of children who do not exist.[130]

The Court concluded that these images do not involve, let alone harm, any children in the production process.[131] In reaching its conclusion, the Court rejected the Government's arguments that pornographic images created without using actual children can encourage pedophilic activity or be used to lure children into performing sexual acts.[132] With respect to these allegations, the Court found the link between sexually explicit images created using adults who looked like children or using computer-generated graphics and the potential for crime was "contingent and indirect."[133] Accordingly, the Court concluded that the Government's interest in preventing production of these images was inadequate to overcome the First Amendment's protections.

These three cases demonstrate governmental and societal interest in protecting children from sexually explicit Internet sites and how the Courts are struggling to balance the first amendment and laws governing the Internet. Since the Internet has been in existence for only the last thirty years, there is a definite possibility that more legislation will be proposed to regulate the Internet and eventually, the Supreme Court may affirm censorious legislation. Until then, it is apparent from these cases that the Court continues to grapple with the issue of how far it should go in regulating the Internet. Furthermore, subject of this paper, the proposed Act, wants to democratize the Internet to the world, yet it is apparent

129. 18 U.S.C. § 2256(8) (2000).
130. *See* Free Speech Coalition, *supra* note 8.
131. *Id* at 248.
132. *Id.*
133. *Id.* at 250.

from these Supreme Court cases and the legislation reviewed that the United States itself deems it necessary to restrict and or regulate certain "information" within our own borders.

IV. IMPACT

This section will address the legislative conflicts that will illustrate why the Act will most likely be unsuccessful. These conflicts are products of domestic regulation as evidenced by enforcement of Internet legislation as seen in the music and gambling industries, powerful lobbyists of corporate America and public policy conflicts, particularly concerning current global image of America. Further, this section will highlight an alternative resolution to the issue of a global Internet and discuss why the ultimate goal of the legislation is crucial in light of current news regarding the outbreak of Severe Acute Respiratory Syndrome ("SARS").

A. Regulation and Enforcement on the Internet

Additional cases on Internet jurisprudence in the U.S. illustrate a requirement for domestic regulation of the use of the Internet. In the U.S., the courts and law enforcement are attempting to regulate the actions of Internet companies such as Napster Inc., and eradicate illegal activity such as Internet gambling. In Time Magazine, reports of some 2.6 billion files are downloaded each month illegally, which has become an enormous financial liability for the entertainment industry.[134] These crimes are prevalent and the entertainment industry is fighting back in the courts. In addition, law-enforcement agencies are currently approaching credit-card companies and other online payment vehicles that make online gambling possible.[135]

---

134. Lev Grossman, *Music? Movies? TV shows! Millions of people download them everyday. Is digital piracy killing the entertainment industry?*, TIME, May 5, 2003, at 60.

135. Michael Totty, *Regulations: Taming the Frontier*, THE WALL STREET JOURNAL, January 27, 2003, at R10.

In 2001, Napster Inc.'s evolving technology, which capitalizes on peer-to-peer architecture,[136] was ordered by the courts to close its doors based on copyright infringement violations. File-sharing software takes advantage of the fact that music and movies are stored as digital data, and are not vinyl and celluloid anymore. Rather, they are collections of disembodied, computerized bits that can be stored or played on a computer and transmitted over the Internet as easily as e-mail.[137] Websites that provide file sharing, popular on college campuses and high schools, allow users to download video, music and software for free at high speeds. In this landmark case, *A&M Records, Inc. v. Napster, Inc.*, [138] the U.S. Court of Appeals ordered the closing of the website until new filtering devises were installed. This was a huge success for the U.S. recording industry, but a small battle in a war they are currently losing.

The recording industry's success in shutting down Napster in 2001 has sent consumers to other file-sharing services such as Kazaa, Gnutella and Direct Connect.[139] These file-sharing services are smarter and more decentralized then Napster whose network relied on a central server, an Achilles' heel that made it easer to unplug and shut down.[140] For example, Kazaa, the most popular file-sharing software, is built around a floating, distributed network of individual PC's that has no center.[141] In addition, Kazaa has chosen a decentralized business strategy too: it is a mirage of complicated partnerships with the official owner, Sharman Networks, tucked away on the South Pacific island of Vanuatu.[142] So far, this diffused structure has kept management off U.S. soil and out of U.S. courtrooms.[143]

It is apparent that this will be a future legal dilemma that the

136. *See supra* text accompanying note 52.
137. *See* Grossman, *supra* note 134.
138. A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2001).
139. *See* Grossman, *supra* note 134.
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*

courts will have to deal with as large recording companies continue to lose money. According to Jack Valenti, head of the Motion Picture Association of America ("MPAA"), views on illegal downloading, "if we let this stand, you're going to see the undoing of society."[144] All the while it is reported that pirates swap between 400,000 and 600,000 movies online everyday and CD shipments last year were down 9% on top of a 6% decline in 2001.[145] These facts represent a significant problem for the entertainment industry that remains determined to fight each step in the courts to restrict Internet file sharing.

In some cases, enforcing law and order on the Web is just as difficult as in the physical world. Illegal gambling over the Internet is prevalent with the latest estimates of about $3.5 billion being wagered this year on some 1,800 Internet gambling sites, most located in Costa Rica or other offshore locations.[146] Even though this is illegal in most states, online gambling sites get about 60% of their revenue from the U.S.[147] As a result, law-enforcement agencies have narrowed in on the weakest link of the transactions and started to investigate and prosecute credit-card companies and other online payment vehicles that make online betting possible.[148]

For example, New York Attorney General Eliot Spitzer forced Citigroup Inc.'s Citibank, the nation's largest credit-card issuer, to agree to quit taking charges from online bets last summer.[149] There is also pressure on online payment service PayPal, a unit of eBay Inc., by Mr. Spitzer, which resulted in the service agreeing to prevent New York residents from using it to gamble online.[150] This current trend demonstrates a governmental interest in

144. *Id.*

145. *Id.* In 2000 the top 10 albums in America sold 60 million copies; in 2001, 40 million; in 2002, 33 million.

146. *See* Totty, *supra* note 135.

147. *Id.*

148. *Id.*

149. *Id.*

150. *Id.* At least 400 banks that issue MasterCard and Visa credit cards have refused to honor online bets; not because they fear the wrath of the law enforcement, but because in many states they cannot rely on the law to go after deadbeats.

regulating access on the Internet and enforcing barriers to prevent them from participating in these acts. This enforcement seems to be semi-successful, but at the same time, how does the U.S. have authority to enforce the proposed Act in other countries, which is intended to liberalize Internet censorship?

With domestic issues enforcing violations of copyright infringement over the Internet, it is difficult to balance this new legislation in Congress. The Act's purpose is two-faced to the current trends in domestic policy over the Internet. The bill does explicitly state that it will not be used to interfere with legitimate law-enforcement aims; however, the bill does not define what legitimate means in connection with the law of other countries. If legitimate is what the U.S. views as legitimate, then it will be discretionary and the effects of the bill could travel down a very slippery slope. According to Nail Al-Jubeir, a spokesman for the Saudi Embassy, "this legislation is culturally arrogant. Each society has its own standards. Ours are different from everybody's."[151]

B. The Lobbying Powers of Large Corporations

The United States is a capitalist society that engages in business all over the world. There are many alliances worldwide, but one of the largest growing markets with the most potential is Asia. Recently, Amnesty International, an human rights group, publishes a list of corporations that they consider violate the goals of a free Internet.[152] The Act also proposes to produce a similar list that will be published in their annual report to Congress that may potentially pressure Western companies to stop providing their services and products to countries that use them to censor the Internet.[153]

---

151. Luciana Lopez, *Anti-jamming Bill Faces Stiff Obstacles: Opponents Call It Unenforceable*, THE WASHINGTON TIMES, November 4, 2002, at 16.

152. *See supra* text accompanying note 83.

153. H.R. 48 § 4(d), which states "Each report shall list the countries that pursue policies of Internet censorship, blocking, and other abuses; provide information concerning the government agencies or quasi-governmental

It is very apparent that technology has made a tremendous impact on society and indirectly on human rights. Currently, many Western companies have formed profitable business partnerships with countries such as China to provide technical support that results in China being able to enforce its' repressive Internet regulations. In addition, it is reported that China's expanding technology market is worth more than $20 billion a year and with slumping sales domestically, Western corporations need that available market in order to continue their growth.[154]

C. The Global Image of America – Interventionist Attitudes

It is apparent from global publications that the United States is currently not very well received internationally.[155] According to a Time article, "humility, not hubris, is crucial to winning the peace" in Iraq.[156] Moreover, U.S. current political moves regarding the war in Iraq, have left many negative impressions on the world. In Asian Political News, on the topic of U.S. global image, "it is unclear whether the current anti-Americanism is going to be short-lived or go on for a long haul, but the U.S. as a country is being perceived, perhaps wrongly, as a bully because of the hawkish dominated White House."[157] With this Act, the U.S. is risking perpetuating a perception that it is continuing its interventionist attitudes and imposing their views on what should and should not be censored.

The 2003 War in Iraq has potentially caused irreconcilable harm to the image of America abroad. With the War, the American government must be weary of its actions that will affect those abroad and continue to forge current and new alliances with

---

organizations that implement Internet censorship; and ***describe with the greatest particularity practicable the technological means by which such blocking and other abuses are accomplished***. In the discretion of the Director, such report may be submitted in both a classified and nonclassified version."

154. *See* Mooney, *supra* note 36.

155. Joe Klein, *America Shows Its Colors*, TIME, March 31, 2003, at 198.

156. *Id.*

157. *Asian Editorial Excerpts*, ASIAN POLITICAL NEWS, April 7, 2003.

foreign countries. In addition, these negative foreign attitudes will cause irreconcilable economic harm to U.S. companies and their brands abroad, such as McDonalds and Starbucks.[158] Furthermore, with political unrest and tension in North Korea, it is apparent that the U.S. should not jeopardize its current relations with China.

By enacting this Act, the U.S. would jeopardize relationships with several foreign countries, but most importantly with China. Ultimately, this is not the correct political move for the U.S. as they exit the battlefield and enter the hazardous stage of repairing their global public image, now overshadowed by unilateralism.[159]

D. Legislation as an Advisory Function

International human rights are taken for granted by some in the U.S. and it is apparent that with the intense growth of technology and the Internet, these rights are being stricken from many people on the global level. This is an issue that multi-national organizations, such as the United Nations, should investigate and report. Human rights are a global issue that should not be left to one nation to regulate. The United Nations should be given the power to sanction those countries in violation of human rights norms and pressure countries that aid in the process. In addition, the U.S. should still publicly condemn violations committed in China, but promote more international organizations to enforce legislation such as this Act.

It is apparent form the SARS outbreak in Asia that if information were not censored, lives could have been saved. Recently, SARS was the second-most searched phrase on Yahoo.[160] However, it is apparent that this information was kept away from Internet surfers in China. Many blame the spread of SARS on China's refusal to accept that the disease was a problem last year, and refused to call in international experts to help

158. *Id.*

159. *Id.*

160. Melody Petersen, *A Respiratory Illness: Cashing In*, THE NEW YORK TIMES, April 14, 2003, at §A p12.

identify and contain the disease.[161]

The depth of the misinformation campaign became clear in early April, when Health Minister Zhang Wenkang scoffed at members of the World Health Organization ("WHO") warnings against travel to southern China and declared, "it is perfectly safe" to visit the country.[162] It is reported as a result of this outbreak, some China watchers believe that the public clamor for transparency may create an opportunity for China's new President, Hu Jintao, a career bureaucrat with liberal tendencies, to push for the kinds of sweeping political reforms that party elders have long resisted.[163]

Accordingly, if democracy advocates want to promote meaningful change, they must also recognize the Internet's ability to change authoritarian regimes from within.[164] As nations such as China embrace the Web to streamline government and boost economic growth, they also create opportunities for greater transparency, accountability, and freedom.[165] Ultimately, repressive regimes are forced to choose between jumping on the information superhighway or languishing on the unwired byways of technology.[166] Many of these regimes are choosing to go along for the Internet ride because, in addition to helping leaders compete in the global economy, the Internet and other information communication technologies can streamline authoritarian states and help them govern more effectively, which is attractive options for many leaders.[167]

Once strong-arm regimes open the door to technology, they may find it difficult to return to a culture of bureaucratic secrecy,

---

161. David Wall, *Chinese Deserve Grown-up Party Leaders*, THE JAPAN TIMES, April 13, 2003.

162. Romesh Ratnesar and Hannah Beech, *Tale of Two Countries*, TIME, May 5, 2003, at 55.

163. *Id.* at 56.

164. Shanthi Kalathil, *Dot com For Dictators*, Internet Use to Challenge Authoritarianism, Carnegie Endowment for International Peace Foreign Policy, March 1, 2003 at 43.

165. *Id.*

166. *Id.*

167. *Id.*

unscrupulous abuse of power, and unaccountability.[168] Furthermore, aid organization and Congress need to be aware of these activities and if an Office of Global Internet Freedom is to be established, it should have as its mandate not merely unjamming Web sites, but also coordinating various government efforts to better achieve democratic reform.[169]

V. CONCLUSION

The Internet can certainly "free" people to interact worldwide with others, but to what ends is often unclear. However, if these ends become reasonably clear, they may be unsettling. Extreme Internet communities, obscene materials, and child pornography are to most, disturbing activities on the Internet, yet to some libertarians these are empowering acts of speech that are protected under the First Amendment. Free Speech is a powerful tool that Americans and the courts are constantly struggling to redefine. This Act before Congress hopes to free the Internet on an international scale by creating a Committee that will aid and fund individual human right activists. Unfortunately, this legislation will probably be unsuccessful due to questionable domestic regulation and enforcement of the Internet, powerful opposition by corporations, and the need to repair the U.S. international public image.

Unlike World War II and the Voice of America, we live in an international community that is not at war with countries in violation of censoring the Internet. In the end, enforcement of this legislation should be administered by international organizations, such as the United Nations, because freedom of speech is an important right and is essential to any form of democracy.

Elaine M. Chen

168. *Id.*
169. *Id.*