San Diego Law Review

Volume 45 | Issue 1 Article 7

2-1-2008

Speak No Evil: Circumventing Chinese Censorship

Jennifer Shyu

Speak No Evil: Circumventing Chinese Censorship

JENNIFER SHYU*

TABLE OF CONTENTS

* J.D. Candidate 2008, University of San Diego School of Law; B.A., Molecular and Cell Biology, 2003, University of California, Berkeley. Special thanks to Professor Jane Henning for her guidance and advice, and to my Comment Editor Christine Yung for her encouragement and support. I would also like to thank my dear friend Crispin Van Buer who suffered with me throughout the writing process.

I. INTRODUCTION

On February 15, 2006, the House Committee on International Relations invited executives from Google, Inc., Microsoft Corp., Yahoo!, Inc., and Cisco Systems, Inc. to what was supposed to be a "discussion" about these American corporations' cooperation with China to enforce Chinese Internet censorship and persecute China's political dissidents.[1] Instead, Congressman Christopher Smith (R-NJ) launched a scathing attack on the executives, listing names of dissidents jailed for their Internet postings and reminding the corporations of their roles in the dissidents' captures.[2] Congressman Smith next accused Google of compromising its do-no-evil policy by bowing to the will of China's oppressive government.[3] Congressman Smith also compared the corporations to IBM in Nazi Germany and alleged, "U.S. technology companies today are engaged in a similar sickening collaboration, decapitating the voice of the dissidents."[4] Congressman Tom Lantos (D-Cal.) summarized the reason for the hearing: "What Congress is looking for is real spine and a willingness to stand up to the outrageous demands of a totalitarian regime. Your abhorrent activities in China are a disgrace."[5]

During the ensuing interrogation, the corporations attempted to defend their actions by arguing they picked the lesser of two evils: complying with Chinese law by censoring the Internet, instead of leaving the Chinese market altogether and thus allowing the Chinese search engines to conduct their own censorship, presumably more rigorously than their

1. *See The Internet in China: A Tool for Freedom or Suppression?: Joint Hearing Before the Subcomm. on Africa., Global Human Rights and Int'l Operations and the Subcomm. on Asia and the Pacific*, 109th Cong. (2006) [hereinafter *Hearing*].

2. These include online posters Li Zhi and Shi Tao, who drew eight and ten years respectively in prison for expressing their opinions on the Internet. Yahoo! Inc. provided the Chinese government with the physical location of these online posters. *Id.* at 1–2, 10 (statements of Rep. Christopher Smith, Chairman, H. Subcomm. on Africa, Global Human Rights and International Operations and Rep. James Leach, Chairman, H. Subcomm. on Asia and the Pacific). In addition to Yahoo!'s cooperation with the Chinese government in enforcing China's Internet censorship regulations, Google stands accused of censoring its search engine at the request of the Chinese government, Microsoft of censoring personal websites by Chinese citizens that express opinions contrary to that of the government, and Cisco Systems (an Internet hardware company) of providing the Chinese government with the technology necessary to control the Internet. *Id.* at 3.

3. *Id.* at 3.

4. His reference here is from Edwin Black's book documenting how IBM knowingly provided Nazi Germany with the ability to operate at "Blitzkrieg efficiency." *Id.* at 2 (statement of Rep. Christopher Smith); *see* EDWIN BLACK, IBM AND THE HOLOCAUST 203 (2001); *see also* THE CORPORATION (Zeitgeist Films 2004) (exploring IBM's role in aiding Nazi Germany). In its own defense, IBM states that the Nazi party, apart from IBM, controlled IBM's German subsidiary.

5. *Hearing*, *supra* note 1, at 8 (statement of Rep. Tom Lantos, Member, H. Subcomm. on Africa, Global Human Rights and International Operations).

American counterparts.[6] Congressman Lantos, however, addressed the executives in plain speech, asking each if he was ashamed of the actions of each corporation or could see the similarities between the corporation's actions and that of IBM in aiding Nazi Germany.[7] The executives avoided the question.[8]

After Congressman Lantos concluded his inquiry into the morality of their actions, Congressman Brad Sherman (D-Cal.) addressed the legal issue:

> [W]hat have you done to tell your Chinese customers that they have a lower expectation of privacy and that you will comply not with the law of your democratically elected host government, namely the United States, but rather

---

6. From the hearing transcript, edited for clarity:

> [YAHOO] Our belief, Mr. Congressman, is that the benefits of having access to communication service, as well as access to independent sources of information, coupled with the extreme large number of searches and other activity that happens on the Web, provides an extraordinary benefit. We recognize these extreme challenges as well, and we are ready to tackle those, along with our industry peers and with government, in partnership to make this a government-to-government dialogue.
>
> [MICROSOFT] I would just reiterate that we think these are very difficult issues, which I think is clear from some of the questions from the Members, but we, too, think, on balance, that it is better for Microsoft and the other companies here at the table and other United States Internet companies to be engaged in China. We think that the benefits far outweigh the downside in terms of promoting freedom of expression.
>
> [GOOGLE] We made the decision to enter the market because we believe in making information available and accessible. We believe that doing that will achieve positive things. As I said in my testimony and in my oral statement, if, over time, we do not achieve the results that we seek, because your question is a legitimate one, we will reconsider our role there.
>
> [CISCO] The Internet is many different things to different people. For some, it is a source of empowerment, enlightenment, giving them access to information they never had before. Others are frightened by that empowerment and see nonstate actors, whether they are multinational corporations or terrorists or antiglobalization activists, empowered against legitimate state authority, and others see the Internet being used as a tool of repression. I think all of those are correct.

Id. at 90. For the opposing view that globalization alone is enough to bring democracy and freedom to less democratic governments, see THOMAS FRIEDMAN, THE WORLD IS FLAT: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY 10 (2005) (claiming that globalization has "made us all next-door neighbors").

7. "Can you say in English that you are ashamed of what you and your company and the other companies have done? . . . IBM complied with legal orders when they cooperated with Nazi Germany. . . . [D]o you think that IBM, during that period, had something to be ashamed of?" *Hearing*, *supra* note 1, at 97–98 (statement of Rep. Tom Lantos).

8. *Id.*

> that you will furnish information upon the request of an un-elected, un-democratic and oppressive government in China?[9]

This Comment will focus on the issue of the role of American corporations in enforcing Chinese censorship law.

In the hands of the Chinese government, the increased freedom of speech granted by the Internet and brought to China via American corporations is curtailed by state-sponsored censorship. To do business in China, American companies must comply with Chinese Internet censorship laws, yet these very laws not only restrain the freedom of speech of Chinese citizens but also subject offenders to the whim of the Chinese secret police. As accurately stated in the hearing, Yahoo! aided China in arresting at least two Chinese online writers for the crime of disagreeing with the government.[10] The United States must act to stop American corporations from further participating in China's persecution of its political dissidents.

At the conclusion of this hearing, Congress proposed a possible solution in the Global Online Freedom Act, a bill that would reach and punish American companies engaged in enforcing Chinese state-sponsored censorship.[11] Although the bill embodies ambitious ideals, as this Comment explains, its passage forces other nations to follow United States law wherever private United States companies operate.[12] Instead, Congress should examine additional short-term solutions that avoid imposing American law onto another sovereign nation and circumvent unresolved issues of international Internet regulation.[13]

Part II of the Comment briefly surveys the history of the Internet, focusing on previous attempts at Internet regulation, both domestic and foreign. It will highlight the social causes of these regulations and explore the results when social values in one country do not comport with the values in another. Part III addresses the Global Online Freedom Act, particularly its purpose, provisions, and criticisms. This Part also considers alternative short-term solutions to this bill that avoid the

---

9. *Id.* at 117. Here, Congressman Sherman uses the term *expectation of privacy* not in a legal sense, but in a colloquial sense to convey that the corporations do not afford equal treatment to Chinese citizens, as opposed to American customers.

10. *See* Amnesty International, *Undermining Freedom of Expression in China*, July 2006, http://web.amnesty.org/library/Index/ENGPOL300262006.

11. Global Online Freedom Act of 2006, H.R. 4780, 109th Cong. (2006); Global Online Freedom Act of 2007, H.R. 275, 110th Cong. (as reported by H. Comm. on Foreign Affairs on Dec. 10, 2007).

12. *See infra* Part III.A.

13. The best long-term solution to this conundrum would be the enactment of international Internet regulations. However, this Comment will not explore in depth this much larger and more complex question of whether worldwide Internet laws should be enacted and whether the Internet should even come under international control.

blatant interjection of United States law into another sovereign state and analyzes the viability and requirements for the success of these solutions in China. Part IV follows with a final recommendation of the best course of action at this time: the promotion of proxy-blocking Internet services coupled with the economic pressure of the international community to force China to cease persecution of its online political dissidents.

II. BACKGROUND

A. The Initial Promise of the Internet

In 1969, the United States military envisioned a system that could link military, defense, and university members engaged in defense research.[14] From this vision, the Defense Advanced Research Project Agency (DARPA) invented the ARPANET (Advanced Research Project Network), the early precursor to the Internet.[15] The ARPANET consisted of an intangible network connecting innumerable smaller groups of computer networks.[16] ARPANET facilitated the decentralized and rapid transmission of information from individual to individual.[17] As it grew in use and popularity, networks similar to ARPANET sprung up, linking businesses, universities, and research facilities around the world.[18] Eventually these networks merged together into what is known today as the Internet.[19] In the 1980s, the Internet experienced extraordinary growth so that today the Internet connects one billion users from every country in the world.[20]

The secret of the Internet's success has remained unchanged from its inception to present time; as a completely decentralized, self-maintaining entity, the control of information lies in the hands of each user.[21] Whatever each user chooses to view, publish, or discuss defines the boundaries of that user's cyberspace.[22] Moreover, Internet information dwells in this

14. ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997) (summarizing the creation and development of the Internet).
15. *Id.*
16. *Id.*
17. *Id.*
18. *Id.* These networks included BITNET, FIDONET, and USENET. *Id.*
19. *Id.*
20. Internet World Stats is commonly cited authority on Internet usage by country and worldwide. Internet World Stats, http://www.internetworldstats.com.
21. *ACLU*, 929 F. Supp. at 831, 838.
22. *Cyberspace*, the term now used almost synonymously with *Internet* to describe that nebulous realm where humans can gather to exchange ideas, was originally coined

cyberspace—inside an intangible realm that has no centralized storage location or control point.[23] Consequently, it eludes the control of any single business, individual, or country.[24]

The Internet's power stems from its ability to grant an unprecedented forum for free speech.[25] Using the Internet, users can communicate via email, bulletin boards, public forums, and chat rooms.[26] More recently, web blogs have surged in popularity, significantly adding to the amount of personal websites. In addition, the convenience and affordability of the Internet allows almost any individual with a computer and network connection to broadcast opinions and thoughts worldwide.[27] The resulting erasure of the lines defining race and wealth creates a truly democratic forum. Nongovernmental and political organizations also discovered the Internet's usefulness in championing lesser known causes because it provides a cheap and effective means of reaching target audiences.[28] Even today, some believe democracy will come to China through the inherent properties of the Internet; a generation of Chinese citizens growing up with the ability to exercise unrestricted public speech online every day will set the foundation for a more democratic society.[29]

---

by science fiction author William Gibson. WILLIAM GIBSON, ENCYCLOPEDIA OF NEW MEDIA 112 (2003). He defined cyberspace as a "consensual hallucination." WILLIAM GIBSON, NEUROMANCER 5 (1984).

23. *ACLU*, 929 F. Supp. at 831.

24. *Id.* at 832.

25. As John Perry Barlow, cofounder of the Electronic Frontier Foundation, put it in 1996, "We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before." *See* John Perry Barlow, A Declaration of the Independence of Cyberspace (Feb. 8, 1996), http://homes.eff.org/~barlow/Declaration-Final.html. Barlow's widely circulated sixteen-paragraph Declaration of the Independence of Cyberspace captures the early fascination and excitement of the Internet. *Id*.

26. *ACLU*, 929 F. Supp. at 834; *see also* Elizabeth A. Ritvo, *Online Forums and Chat Rooms in Defamation Actions*, 24 COMM. LAW. 1 (2006) (explaining how the hearsay exceptions can aid plaintiffs in admitting defamatory chat room statements as evidence).

27. *ACLU*, 929 F. Supp. at 838.

28. *See id.* at 842–43. Presidential candidate Howard Dean raised more money than any other Democratic candidate. His fundraising success came as a result of his supporters on the political websites Meetup.com and Moveon.org. *See* Gary Wolf, *How the Internet Invented Howard Dean*, WIRED, Jan. 2004, at 138, *available at* http://www.wired.com/wired/archive/12.01/dean_pr.html. Even the United States government uses the Internet for military recruitment. The Marines use MySpace, a popular social networking site among teenagers and young adults, to direct visitors to its recruitment centers. Their site is located at http://www.myspace.com/themarinecorps (last visited Mar. 14, 2008).

29. Clive Thompson, *Google's China Problem (and China's Google Problem)*, N.Y. TIMES MAG., Apr. 23, 2006, at 156.

B. United States Internet Regulations

Unfortunately, this new medium for free speech ushered in a new era of exploitation.[30] In the United States, the Internet led to the proliferation of child pornography,[31] the defamation of corporations and individuals,[32] and the unmasking and subsequent punishment of anonymous writers.[33] Congress responded to these unforeseen issues by encouraging the privatization of parts of the Internet, effectively bringing those parts outside the reach of the First Amendment.[34] To protect the American public, Congress passed laws regulating the public aspects of the Internet. However, the Supreme Court has consistently used the First Amendment to strike down these statutes.

To ban online access to child pornography and to protect minors from "indecent" and "patently offensive" materials, Congress passed the Communications Decency Act of 1996 (CDA).[35] The CDA criminalized the use of a computer to display or send comments, images, or

30. *See ACLU*, 929 F. Supp. at 824, 844.

31. For an overview of the difficulties in enforcing child online pornography in the United States and overseas, see Alexander Shytov, *Indecency on the Internet and International Law*, 13 INT'L J.L. & INFO. TECH. 260 (2005) (discussing differences in laws, culture, and opinions between countries as to how best to deal with online child pornography).

32. Websites such as Don't Date Him Girl, http://www.dontdatehimgirl.com/home/ (last visited Mar. 14, 2008), allow users to warn others about bad dates, often identifying the date by real name or screenname. A Pittsburgh resident sued the site for defamation after users labeled him a homosexual and a carrier of sexually transmitted diseases. On April 5, 2007, a Pennsylvania court dismissed his case for lack of jurisdiction. *See* Memorandum and Order of Court, Hollis v. Joseph, No. GD06-012677 (Pa. D. & C. Apr. 5, 2007), *available at* http://howappealing.law.com/ 2007040910031 8184.pdf; *see also* Lizette Alvarez, *(Name Here) is a Liar and a Cheat*, N.Y. TIMES, Feb. 16, 2006, at G1.

33. Perhaps the most well-known anonymous website on the workings of the federal judiciary, Underneath Their Robes, turned out to be the work of an assistant United States attorney. Once his identity was discovered, the site was removed. *See* Adam Liptik, *Mystery of Gossipy Blog On the Judiciary Is Solved*, N.Y. TIMES, Nov. 16, 2005, at A14.

34. *See generally* Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115 (2005) (discussing the increasing regulations on the previously unregulated areas in cyberspace of chat rooms and discussion boards).

35. *ACLU*, 929 F. Supp. at 849–50. Had it passed in its entirety, the CDA would have been codified at 47 U.S.C. § 223(a)–(h). *Id.* at 827 n.1. However, the court only struck out the offending provisions; the other parts of the CDA were signed into law and are scattered throughout the Code.

communications deemed patently offensive, as determined by contemporary community standards.[36]

On the day President Clinton signed the CDA into law, the American Civil Liberties Union (ACLU) and eighteen other mostly nonprofit organizations filed suit claiming that the statute violated the First Amendment's right to freedom of speech.[37] The case went to the Supreme Court where the plaintiffs ultimately prevailed. The Court, troubled by the lack of definitions for the terms *indecent* and *patently offensive*, and by the government's use of the terms interchangeably in the statute, ultimately ruled these sections of the CDA to be overly broad and therefore unconstitutional.[38]

In making its ruling, the Court relied on the opinion of the district court,[39] which in turn relied heavily on this nation's historical deference to First Amendment rights.[40] The district court found the CDA was not narrowly tailored to warrant such a "patent intrusion on a substantial category of protected speech for adults."[41] The "loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury."[42]

This deference to First Amendment rights continued in *Ashcroft v. ACLU*.[43] In response to the defeat of the CDA, and to answer continuing public concern regarding online child pornography, Congress passed the Child Online Protection Act (COPA) in 1998.[44] *Ashcroft v. ACLU* involved COPA's criminalization of those who knowingly posted

---

36. *Id.* at 829.

37. *Id*. at 827 n.2. In addition to the ACLU, the plaintiffs included Human Rights Watch, Electronic Privacy Information Center, Electronic Frontier Foundation, Stop Prisoner Rape, AIDS Education Global Information System, Planned Parenthood, Journalism Education Center, and many more. *Id.*

38. Reno v. ACLU, 521 U.S. 844 at 870–71 (1997). *Compare* 47 U.S.C. § 223 (2003), *with* 47 U.S.C. § 223 (2000) (demonstrating Congress amended the CDA in 2003 to remove the offending sections).

39. *See* ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

40. This deference is present in prior court opinions. The Supreme Court has stated that "in spite of the probability of excesses and abuses, these liberties are . . . essential to enlightened opinion and right conduct on the part of citizens of a democracy." New York Times v. Sullivan, 376 U.S. 254, 271 (1964) (quoting Cantwell v. Connecticut, 310 U.S. 296, 310 (1940)).

41. *ACLU*, 929 F. Supp. at 855 (agreeing with plaintiffs that a ban on patently offensive materials would hinder campaigns against genital mutilation and prison rape).

42. *Id.* at 851 (citing New York Times Co. v. United States, 403 U.S. 713 (1971)).

43. Ashcroft v. ACLU, 542 U.S. 656 (2004).

44. 47 U.S.C. § 231 (2000), *invalidated by* ACLU v. Gonzales, 478 F. Supp. 2d 775 (E.D. Pa. 2007). The legislative findings in COPA state: "[T]he protection of the physical and psychological well-being of minors by shielding them from materials that are harmful to them is a compelling governmental interest." Child Online Protection Act, Pub. L. No. 105-277, § 1402, 112 Stat. 2681-736 (1998).

online content harmful to minors for commercial purposes.[45] Unlike the CDA, COPA defined commercial purpose and allowed an affirmative defense to those who use specified means to prevent minors from accessing a particular website.[46] Even these details, however, failed to satisfy the Supreme Court. Despite an affirmative defense, speakers may still censor themselves rather than face possible prosecution, resulting in "extraordinary harm" and causing a "serious chill upon protected speech."[47]

This clash between restricting child exploitation on the Internet and preserving the Internet's promise as a forum for free speech continues today. The House of Representatives recently introduced the Deleting Online Predators Act of 2007 (DOPA).[48] DOPA would force federally funded libraries to block any "commercial social networking website or chat room," ideally to prevent students from entering into chat rooms at school and potentially conversing with sexual predators.[49] Like the CDA and COPA, however, DOPA's main problem may be its broad definition of "commercial social networking sites."[50] This bill may or may not move on to the Senate to continue the debate.[51]

---

45. *Ashcroft*, 542 U.S. at 659–60.

46. 47 U.S.C. § 231(e)(2). "Specified means" include restricting access to minors by requiring any of the following: a credit card, debit account, adult access code, digital certificate verifying age, or "any other reasonable measures that are feasible under available technology." *Id.* § 231(c)(1).

47. *Ashcroft*, 542 U.S. at 671. The Court agreed with the Third Circuit's decision in finding that COPA was not the least restrictive means of protecting minors from harmful websites but remanded the case for proceedings consistent with the reasoning of the Court. *Id.*

48. Deleting Online Predators Act of 2007, H.R. 1120, 110th Cong. § 2 (2007) ("[O]ne in five children has been approached sexually on the Internet.").

49. *Id.* § 3(b)(i)(II). Common social networking sites include MySpace.com, http://www.myspace.com (last visited Mar. 14, 2008), and Facebook.com, http://www.facebook.com (last visited Mar. 14, 2008). In 2006, MySpace had an estimated worth of $2 billion. Andrew Ross Sorkin & Peter Edmonston, *Google Is Said to Set Sights on YouTube*, N.Y. TIMES, Oct. 7, 2006, at C9. In October 2006, Yahoo! reportedly offered to buy the less popular Facebook for $900 million. Saul Hansell, *Yahoo Woos Social Networking Site*, N.Y. TIMES, Sept. 22, 2006, at C1. On a side note, Google has since acquired YouTube for $1.65 billion in stock. Yahoo! reportedly flirted with the idea of buying YouTube but talks broke down. Saul Hansell, *These Days No. 1 Portal Seems to be a Step Behind*, N.Y. TIMES, Oct. 11, 2006, at C1.

50. As defined in DOPA, commercial social networking sites allow the creation of user-specific profiles to participate in forums and chat rooms. H.R. 1120 § 3(c)(J)(ii). However, common websites hosted by Yahoo!, Amazon, and the *New York Times* all allow users to create profiles and participate in online discussions. The passage of this bill could block these sites from school libraries.

51. At the time of this Comment, the bill sits before the House Committee on

The United States' tolerance for racist or Nazi websites, in contrast to foreign countries that censor these sites, further reflects the comparably liberal free speech policy.[52] Perhaps as a result of this policy, defamation law on the Internet remains an area largely unexplored by the courts of this country. In *Gertz v. Welch*, the Court carved out an exception to the right to free speech, protecting private individuals from defamatory accusations.[53] However, lawsuits concerning defamatory accusations on the Internet have only just begun to surface.[54] It appears unclear whether the Court will treat defamation on the Internet in the same manner as defamation in print media.[55]

Energy and Commerce. MySpace, though, has taken the initiative to implement new technology that will compare its user names with a registry of sex offenders in an attempt to protect the minors who use MySpace's services. Matt Richtel, *MySpace.com Moves to Keep Sex Offenders Off of Its Website*, N.Y. TIMES, Dec. 6, 2006, at C3. While not a foolproof strategy, MySpace has at least shown Congress that private industry can regulate itself.

52. A search for Nazi, white supremacist, or racist sites on a search engine targeted at the United States audience (such as http://www.yahoo.com) will yield positive results, whereas such a search on a French website (like http://www.yahoo.fr) will not.

53. *See* Gertz v. Welch, 418 U.S. 323, 345 (1974) (differentiating between the expectation of privacy between public figures and private individuals).

54. In *Dow Jones & Co. v. Gutnick*, an Australian citizen sued the American company, Dow Jones, in Australia after an allegedly defamatory article appeared on the Dow Jones' subscriber-only website. (2002) 210 C.L.R. 575 (Austl.). Dow Jones argued that because the defamatory materials were published on servers in the United States, Australia lacked jurisdiction. *Id.* at 579. However, the High Court of Australia disagreed, holding that the moment of publication occurred when Australian users downloaded the materials from the server. *Id.* at 587–88. Thus, Australia had proper jurisdiction and the court ruled in favor of Gutnick. The High Court further noted that it is the place of the legislature to reform the common law of defamation. *Id.* at 600–01. Absent action on that front, the High Court would apply the traditional legal doctrines towards Internet cases. *Id.* at 607; *see also* Michael Saadat, *Jurisdiction and the Internet after Gutnick and Yahoo!*, J. INFO. L. & TECH. (2005), *available at* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2005_1/saadat (considering the jurisdictional issues associated with the Internet, particularly with respect to defamation). In contrast, the California Supreme Court recently ruled that no provider or user of an interactive computer service may be held liable for putting material authored by a third party on the Internet. Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006). Specifically, the court held that individual posters on websites, newsgroups, search engines, and blogs are protected under Section 230 of the Communications Decency Act of 1996, which explicitly states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." *Id.* at 522–23.

55. Professor Jack Goldsmith argues, "Cyberspace transactions are no different from 'real-space' transnational transactions. They involve people in real space in one jurisdiction communicating with people in real space in other jurisdictions in a way that often does good but sometimes causes harm." Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1250 (1998). However, Professor David Post emphasizes the counter view that the jurisdictional questions raised by the Internet have no real world counterpart and, as a result, traditional legal tools may not apply. David G. Post, *Against "Against Cyberanarchy,"* 17 BERKELEY TECH. L.J. 1365, 1387 (2002).

In instances where the public and private domains overlap, free speech on the Internet is generally not protected. Employees that participate in forums or maintain blogs to discuss work may be fired for their posts.[56] Courts grant little recourse in such situations, even if the employee's website does not discuss trade secrets but merely ridicules his boss.[57] Although unexplored in this country, a lawsuit from a fired blogger against his employer has surfaced in France.[58] This is an area of law that is undergoing development.[59]

C. Internet Regulations in Other Countries

While the United States focused on regulations pertaining to child pornography and free speech, other countries focused on protecting the values embodied in their own cultures. Stemming from the Nazi experience in World War II, French law prohibits Holocaust-denying, racist, Nazi-apologetic, and hate speech websites.[60] Germany has similarly tough laws against racist, anti-Semitic, and white supremacist sites.[61] Reflecting the teachings of modesty in women in Islam, Saudi Arabia blocks sites considered harmful to Muslim culture and values.[62] The

56. A number of bloggers have been fired for blogging at work. *See, e.g.*, Statistics on Fired Bloggers, http://morphemetales.wordpress.com/2006/10/09/statistics-on-fired-bloggers (Oct. 9, 2006). The international community has only begun to address this issue. In France, a British woman who was fired for maintaining a personal blog at work won her case in French court. *See* Bobbie Johnson, *Briton Sacked for Writing Paris Blog Wins Tribunal Case*, THE GUARDIAN, Mar. 30, 2007, at 20.

57. Companies fear employees will inadvertently disclose trade secrets. *See, e.g.*, Vincent Chiappetta, *Employee Blogs and Trade Secrets: Legal Response to Technological Change*, 11 NEXUS: J. OPINION 31 (2006). The Electronic Frontier Foundation (EFF) is a public interest law firm that champions constitutional rights in cases involving the Internet and provides a guide on blogger's rights. *See* How to Blog Safely (About Work or Anything Else) (May 31, 2005), http://www.eff.org/Privacy/Anonymity/blog-anonymously.php.

58. *See* Angela Doland, *Sacre Blog! Fired Gossip Sues in Paris*, CHI. TRIB., July 21, 2006, at 19.

59. An exploration of relevant domestic cases can be found in Konrad Lee, *Anti-Employer Blogging: Employee Breach of the Duty of Loyalty and the Procedure for Allowing Discovery of a Blogger's Identity Before Service of Process is Effected*, 2006 DUKE L. & TECH. REV. 2, ¶¶ 29–42, http://www.law.duke.edu/journals/dltr/articles/2006dltr0002.html.

60. Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 433 F.3d 1199, 1202–03 (9th Cir. 2006).

61. *See* Amber Jene Sayle, *Net Nation and The Digital Revolution: Regulation of Offensive Material for a New Community*, 18 WIS. INT'L L.J. 257, 268–70 (2000).

62. These are primarily sites with a sexual theme. *See* Privacy International, *Silenced: An International Report on Censorship and Control of the Internet*, Sept. 10,

less than democratic societies of Bahrain, China, Iran, and North Korea infamously censor any critique upon the ruling party.[63] Democratic nations in areas of instability impose stricter Internet regulations in the name of national security.[64]

D. When Regulations Clash

The regulations of each country conflict with each other when confronted by foreign websites, displaying materials legal in one country but illegal in another. The *ACLU* court alluded to this quagmire, noting that foreign materials are often stored on domestic servers but domestic servers had no control over entering foreign content.[65] Currently no international law defines and regulates material on the Internet. Even in the realm of child pornography, an issue subject to universal disapproval, governments face legal difficulties capturing overseas perpetrators.[66]

In the realm of free speech, Germany's and France's laws against online hate and racist speech clash with the free speech policies of the United States. In the 1990s, Germany made numerous attempts to censor foreign neo-Nazi websites.[67] These attempts included pressuring commercial providers to voluntarily censor material, threatening to sue foreign Internet Service Providers (ISPs), and passing laws that expressly allowed for the criminal prosecution of ISP executives.[68] This state-sponsored censorship culminated in the indictment of the head of CompuServe Germany on charges of trafficking child pornography and failing to block neo-Nazi sites.[69] Because CompuServe users could download pornography and view otherwise illegal materials on the web, prosecutors charged the executive with allowing users to circumvent the country's ban on these

---

2003, http://www.privacyinternational.org/survey/censorship/Silenced.pdf. This report examines the state of Internet censorship in various countries throughout the world.

63. *Id.* at 47. North Korea actually has no Internet Service Providers and only permits "a handful of citizens" to go online. *Id.*; *see* Tom Zeller Jr., *The Internet Black Hole That Is North Korea*, N.Y. TIMES, Oct. 23, 2006, at C3.

64. *See Yahoo! Inc.*, 433 F.3d at 1202–03.

65. ACLU v. Reno, 929 F. Supp. 824, 848 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

66. Shytov, *supra* note 31, at 263–64.

67. *See* Informations- und Kommunikationsdienste-Gesetz—IuKDG [Information and Communication Services Act], June 13, 1997, BGBl I at 1120, *available at* http://bundesrecht.juris.de (amending Germany's telecommunications law, including censorship provisions, to hold internet service providers responsible for material which appears on the Internet).

68. *See* Amber Jene Sayle, *Net Nation and the Digital Revolution: Regulation of Offensive Material For A New Community*, 18 WIS. INT'L L.J. 257, 268–69 (2000).

69. *Id.* at 271. In the 1990s, CompuServe was a major player in the ISP industry, competing with AOL. It has since been absorbed into AOL and does not operate under "CompuServe." *See* About CompuServe, http://webcenters.netscape.compuserve.com/menu/about.jsp?floc=DCNav2 (last visited Mar. 14, 2008).

materials.[70] The judge overturned the subsequent conviction, noting that the executive was "a slave of the parent company."[71]

This clash of laws emerged again in France in 2000 in a series of cases between Yahoo! and La Ligue Contre Le Racisme et L'Antisemitisme (LICRA).[72] Yahoo! maintains the portal www.yahoo.com for its users in the United States. For its users elsewhere in the world, Yahoo! maintains a separate site for each country, identified by the two-letter country designation. For example, a user in France would access Yahoo! France at fr.yahoo.com. However, nothing prevents a user in France from entering www.yahoo.com and accessing content directed at United States citizens, just as a user living in California can access fr.yahoo.com. This case arose because French citizens used www.yahoo.com—aimed at American users—to access auctions containing Nazi memorabilia—banned on fr.yahoo.com—in other countries.[73] LICRA sued Yahoo! in the Tribunal de Grande Instance de Paris (Court of Paris) alleging that Yahoo! violated Article R645-1 of the French Criminal Code by allowing French citizens access to these items through fr.yahoo.com.[74]

The Court of Paris ordered Yahoo! to "take all necessary measures to dissuade and make impossible any access" from Yahoo.com to any other site that may be construed as an apology for Nazism or denial of the Holocaust.[75] Further, the court agreed that France could prohibit

70. *See* Edmund L. Andrews, *Germany Charges Compuserve Manager*, N.Y. TIMES, Apr. 17, 1997, at D19.

71. *See* Edmund L. Andrews, *German Court Overturns Pornography Ruling Against Compuserve*, N.Y. TIMES, Nov. 18, 1999, at C4.

72. *See* Yaman Akdeniz, *Case Analysis of* League Against Racism and Antisemitism (LICRA), French Union of Jewish Students v Yahoo! Inc. (USA), Yahoo! France, *Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order 20 November, 2000* (2001), http://www.cyber-rights.org/documents/yahoo_ya.pdf. The original court order in French and English translations are provided in the Appendix to the Complaint for Declaratory Relief, Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001) (No. C-00-21275JF).

73. *See* Akdeniz, *supra* note 72.

74. *Id.* Article R645-1 of the Penal Code prohibits the sale of any Nazi propaganda or artifact. *Id.*

75. *Id.* Yahoo! countered that it directed its services towards United States users, its servers were based in the United States, and this order would be "in contravention of the First Amendment . . . which guarantees freedom of opinion and expression to every citizen." Alternatively, Yahoo! argued that it could not determine the geographic location of every Yahoo! user. *Id.*

Yahoo!'s acceptance of the objected items and websites based on the "ethical and moral imperative shared by all democratic states."[76]

In January 2001, Yahoo! announced that it would ban all Nazi and Ku Klux Klan memorabilia from its auction site, along with any other items "associated with groups that promote or glorify hatred or violence."[77] Although Yahoo! insisted it acted independently of the ruling in Paris, it brought Yahoo! in line with French law.

Yahoo! returned to the United States and asked the court to declare the French order unenforceable in the United States.[78] The court agreed, holding that as sovereign nations, France and the United States may freely make and enforce laws within their respective countries but need not enforce the laws of another country.[79] The court stated that the French regulations would be inconsistent with the First Amendment if mandated by a court in the United States.[80]

On appeal in the Ninth Circuit, the court reversed the decision, finding that Yahoo! failed to show an actual violation of its First Amendment rights.[81] The Court of Paris had ordered Yahoo! to block access to Nazi and hateful memorabilia from French users alone.[82] American users, however, are not targeted by this order. In effect, Yahoo! voluntarily instituted a worldwide block on hate speech and references to Nazism.[83] The Ninth Circuit noted that "as to the French users, Yahoo! is necessarily arguing that it has a First Amendment right to violate French criminal law."[84]

These cases illustrate the clash between sovereign states' interests in protecting the values important to their citizens and the free-flowing democratic nature of the Internet: no country willingly relinquishes its borders. Further, international regulation as to issues concerning extraterritoriality and the ill-defined boundaries of the Internet do not exist.[85] As a result, a company could comply with the laws in its home country, violate the laws in another, and be asked by its home country's court to censor materials around the world.

---

76. *Id.*
77. *Yahoo! Inc.*, 169 F. Supp. 2d at 1185.
78. *Id.* at 1181.
79. *Id.* at 1194.
80. *Id*. at 1192.
81. Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 433 F.3d 1199, 1224 (9th Cir. 2006).
82. *Yahoo! Inc.*, 169 F. Supp. 2d at 1184.
83. *See Yahoo! Inc.*, 433 F.3d at 1223.
84. *Id*. at 1221.
85. However, legal options in the international Internet commerce (e-commerce) setting do exist. *See* Taipo Puurunen, *The Judicial Jurisdiction of States Over International Business-to-Consumer Electronic Commerce from the Perspective of Legal Certainty*, 8 U.C. DAVIS J. INT'L L. & POL'Y 133 (2002).

E. The China Problem

To some extent, every country censors the Internet.[86] Even in the United States, a search for "Kazaa"[87] on Google.com used to return a notice informing users that certain search results had been removed in order to comply with Kazaa's lawsuit against Google pursuant to the Digital Millennium Copyright Act (DMCA).[88] However, China has emerged as the main offender in Internet censorship due to its broad censorship of any "unhappy information" and its harsh consequences for those who violate its censorship laws.[89] Further, while users in democratic countries may have the resources to circumvent the censorship laws of their country, China and its authoritarian government successfully capture and punish many who violate its censorship laws.

The introduction of the Internet in China granted its citizens a level of freedom of communication that the government did not anticipate. Realizing the potential for political upheavals, China passed a complicated and intertwined set of regulations directed at ISPs and citizens alike for the purpose of locating and removing dissidents.[90] In 2000, China's

86. Chilling Effects is a website maintained by the Electronic Frontier Foundation. It lists official government notices from various countries ordering material removed from the Internet to comply with that country's laws. The majority of complaints request Google to remove websites posting materials that violate the DMCA. *See* Chilling Effects, http://www.chillingeffects.org/internation/notice.cgi (last visited Mar. 14, 2008).

87. In early 2000, Kazaa emerged as a peer-to-peer file sharing network allowing users to download copyrighted materials free of charge. *See* Press Release, Sharman Networks, Content Industries and Sharman Networks Settle All Global Litigation (July 27, 2006), *available at* http://www.prnewswire.co.uk/cgi/news/release?id=176141. Kazaa subsequently became the target of copyright infringement lawsuits but settled its cases in 2006. *Kazaa Site Becomes Legal Service*, BBC NEWS, July 27, 2006, http://news.bbc.co.uk/2/hi/technology/5220406.stm.

88. The search of "Kazaa" on Google.com returns the result: "In response to a complaint we received under the US Digital Millennium Copyright Act, we have removed (8) result(s) from this page. If you wish, you may read the DMCA complaint for these removed results." Declan McCullagh, *Google Pulls Links to Kazaa Imitator*, CNET NEWS, Sept. 2, 2003, http://www.news.com/2100-1032_3-5070227.html.

89. For a history of Chinese Internet regulations and the reasoning behind the regulations, see Charles Li, *Internet Content Control in China*, 8 INT'L J. COMM. L. & POL'Y 1 (2003).

90. *See* Greg Walton, *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*, RIGHTS & DEMOCRACY, 2001, http://www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html (exploring current and future Internet regulations in China, including electronic surveillance and censorship). According to the United States Department of State, China is also planning to implement an "email filtration system" that can track and monitor

Ministry of Public Service launched the Golden Shield project, aimed at promoting "the adoption of advanced information and communication technology to strengthen central police control, responsiveness, and crime combating capacity to improve the efficiency and effectiveness of police work."[91] The Golden Shield encapsulates these regulations. It envisions the Internet as a mass surveillance tool, promising immediate Internet access to its citizens and increased police security in exchange for the ability to monitor every citizen.[92] To date, the Golden Shield project allows the Chinese government to track up to 162 million Chinese Internet users.[93] Apart from legal regulations, China also censors the Internet through technology, as evidenced on September 3, 2002. On that date China blocked all access to Google, a popular search engine.[94] In the same way users of Yahoo! France could access materials aimed at American users yet banned in France through Yahoo!, Chinese users of Google could access information about banned topics through sites based in other countries.[95] However, because the search engines had no physical offices inside China, China lacked legal authority to charge these search engines with violations of Chinese law.[96] To prevent its citizens from accessing illegal materials, China simply blocked the search engines.[97] Fortunately, China eventually lifted this block as a result of heavy global opposition to this new policy.[98]

---

individual email accounts. U.S. BUREAU OF DEMOCRACY, HUMAN RIGHTS, AND LABOR, U.S. DEPT OF STATE, 1999 COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES—CHINA (2000), *available at* http://www.state.gov/www/global/human_rights/1999_hrp_report/china.html [hereinafter U.S. BUREAU OF DEMOCRACY].

91. Walton, *supra* note 90. The Golden Shield is a collection of regulations, divided in many stages, aimed at allowing China instant access to the registration of records of each citizen. Leaders also envision cameras at every intersection to improve police response time but also to aid in electronic surveillance of its citizens. *Id.*

92. *Id.*

93. China's state network information center, China Internet Network Information Center (CNNIC), released its 2007 survey of Chinese Internet use. The CNNIC found over thirty-seven million rural users and approximately 125 million urban users. Thus, the Golden shield has the potential of monitoring over 162 million citizens. *See* CNNIC, STATISTICAL SURVEY REPORT ON THE INTERNET DEVELOPMENT IN CHINA (2007), http://cnnic.cn/download/2007/20thCNNICreport-en.pdf. China installed "black boxes" on Chinese Internet service providers to monitor activity within individual email accounts. China also plans on developing technology that can detect and delete "unwanted" emails without the recipient's knowledge or consent. U.S. BUREAU OF DEMOCRACY, *supra* note 90.

94. Thompson, *supra* note 29, at 67–68.

95. Banned topics included any reference to Tiananmen Square, Tibet independence, and the Falun Gong, a group China considers a religious cult. *Id.* at 66, 68.

96. *Id.* at 68.

97. *Id.*

98. *Id.* at 71. In *Who Controls the Internet?*, Professors Jack Goldsmith and Tim Wu argue that the effect of global influence on Chinese telecommunications and security policy may be greatly exaggerated or misinterpreted by Western media. JACK GOLDSMITH &

Despite this retreat, the since dubbed "Great Firewall of China"[99] has continually adapted to rapidly changing technology; each new attempt to circumvent the wall is met with equally dedicated programmers on China's side denying access.[100] The firewall operates on multiple levels of filtration, based on a blacklist of sites and filtered words, as well as filtration based on the originating location and final destination of incoming information.[101] Certain sites that are either difficult to filter or contain large amounts of user-created personal content are blocked completely.[102] Further, China's censorship lacks transparency because the government does not distribute a list of censored topics, nor does the government even admit to censorship efforts.[103] Thus, China has introduced an element of psychological pressure on its citizens to censor themselves as they deem appropriate. Of course, a citizen who violates the vague censorship laws faces legal penalties and perhaps more.

The Chinese realize that their government enforces its censorship laws through the physical punishment of citizens who use the Internet for disapproved purposes. According to Amnesty International, China has imprisoned at least fifty-four citizens for wrongful Internet activity under the country's broad interpretation of its Golden Shield regulations.[104]

TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 89 (2006). In fact, China blocks and filters only what it deems fit. *Id.* As a result, a "government's failure to crack down on certain types of Internet communication ultimately reflects a failure of interest or will, not a failure of power." *Id.*

99. The phrase "Great Firewall of China" first appeared as the title of an article in WIRED magazine, bringing public attention to Chinese Internet censorship. *See* Geremie R. Barme & Sang Ye, *The Great Firewall of China*, WIRED, June 1997, *available at* http://www.wired.com/wired/archive/5.06/china.html.

100. OpenNet Initiative provides a very technological examination of China's Internet censorship capabilities. OpenNet Initiative, *Internet Filtering in China in 2004–2005*, http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf. OpenNet Initiative is a collaborative partnership between three universities which address the increased regional control of the Internet. For a list of banned topics and blacklisted sites, see Thompson, *supra* note 29, at 68.

101. Thompson, *supra* note 29, at 68.

102. An example includes the user-created online encyclopedia Wikipedia. *Id.* at 156. Recently, China relaxed its ban on the English version of Wikipedia. The Chinese version remains inaccessible. Noam Cohen, *Chinese Government Relaxes Its Total Ban on Wikipedia*, N.Y. TIMES, Oct. 16, 2006, at C6.

103. OpenNet Initiative, *supra* note 100, at 52.

104. According to Amnesty International, China also has the largest recorded number of imprisoned journalists and cyber-dissidents in the world. Furthermore, those in prison, like Shi Tao, are reportedly forced to work in harsh conditions and their relatives are questioned daily by police. *See* Amnesty International, *Undermining*

In April 2005, Chinese journalist Shi Tao received a sentence of ten years in prison for an email he authored summarizing a meeting on state propaganda.[105] The case garnered worldwide attention because an American corporation, Yahoo!, facilitated Shi Tao's arrest.[106] Because he sent the email from his Yahoo! account, China requested, and Yahoo! Hong Kong delivered, information on Shi Tao's location.[107] Before this incident, prominent United States companies had always provided the technology behind China's Golden Shield.[108] These companies had also long complied with the censorship laws of the particular country.[109] However, this was the first instance in which a United States company's voluntary compliance with censorship law led directly to the imprisonment of a citizen whose only crime was the exercise of free speech.

In January 2006, attention turned from Yahoo! to Google when Google announced a second version of its search engine specifically for Chinese citizens.[110] Located at Google.cn, this search engine would fully comply with China's censorship laws, erasing links to all sites on the Falun Gong, Tiananmen Square, and anything else banned by the government.[111] Previously, no one nation, business, or person could control the Internet. With Google's help, China solved this conundrum by creating a second Internet, a Chinese Internet, which lies completely within Chinese control.[112] Notably, unlike other regimes mentioned before, China is not trying to censor the Internet by blocking technological progress. Instead it seeks to build and control a technologically advanced, highly sophisticated

---

Freedom of Expression in China 15–16, July 2006, http://web.amnesty.org/library/Index/ENGPOL300262006.

105. *Id* at 15. For general technology-related human rights violations in China, such as jailing citizens who use the Internet to voice criticism at the government, see Human Rights in China, http://www.hrichina.org/public/contents/category?cid=8535 (last visited Mar. 14, 2008).

106. Amnesty International, *supra* note 104, at 15.

107. *Id.* China's Golden Shield laws do not apply to Hong Kong or Macau; as special administrative regions they operate under their own respective legal systems. *See* Keith Bradsher, *Chinese Provinces Form Regional Economic Bloc*, N.Y. TIMES, June 2, 2004, at W7 ("Hong Kong and Macau have been special administrative regions of China since Britain handed over Hong Kong in 1997 and Portugal returned Macau in 1999.").

108. These companies include Cisco Systems and Nortel Networks for hardware, Microsoft for software, and Google and Yahoo! for search engine capabilities. *See* Thompson, *supra* note 29, at 155; *see also* Walton, *supra* note 90.

109. Yahoo! changed its policies to comply with French law. Akdeniz, *supra* note 72, at 4.

110. Thompson, *supra* note 29, at 154–55.

111. *Id.* at 86, 154.

112. While Google operationally controls the actual search engine, China through its firewall controls the output of that search engine. Furthermore, many saw this second search engine, Google.cn, as a renunciation of Google's motto of "do no evil," because the corporation chose to profit at the expense of human expression in a country notorious for its human rights violations. *Id.* at 155.

second Internet. The emergence of this second Internet, coupled with the inextricable role of American corporations in providing China with the infrastructure to restrict Internet access, motivated Congress to call the executives into that infamous hearing in February 2006.

III. PROPOSED SOLUTIONS

A. Global Online Freedom Act[113]

On February 16, 2006, after the acrimonious hearing in the House of Representatives, Representative Christopher Smith (R-NJ) introduced the Global Online Freedom Act of 2006. While that bill never became law, it was reintroduced in similar form on January 5, 2007 as the Global Online Freedom Act of 2007 (Act).[114] This Act aims to "promote freedom of expression on the Internet [and] to protect United States businesses from coercion to participate in repression by authoritarian foreign governments . . . ."[115] The Act hopes to accomplish this goal through: (1) promoting global internet freedom; (2) creating minimum corporate standards for online freedom; and (3) establishing export controls for Internet-restrictive countries.[116] Secretary of State

113. The Global Online Freedom Act is not an original creation. On January 7, 2003, Christopher Cox (R-Cal.) and Tom Lantos (D-Cal.), among others, introduced the Global Internet Freedom Act. *See* H.R. 48, 108th Cong. (2003), *available at* http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.48:. Although identical in purpose to this Act, it would accomplish the goals through consultation with the United Nations and by funding technologies aimed at concealing a user's physical location. H.R. 48, 108th Cong. § 5(2)–(3). Analysis of the Global Internet Freedom Act is provided by Elaine M. Chen, *Global Online Internet Freedom: Can Censorship and Freedom Co-Exist*, 13 DEPAUL-LCA J. ART & ENT. L. 229 (2003). This bill was reintroduced in similar form on February 14, 2006. *See* H.R. 4741, 109th Cong. (2006).

114. *See* Global Online Freedom Act of 2006, H.R. 4780, 109th Cong. (2006); Global Online Freedom Act of 2007, H.R. 275, 110th Cong. (as reported by H. Comm. on Foreign Affairs on Dec. 10, 2007).

115. H.R. 275. Other purposes include promoting the free flow of information and deterring United States businesses "from cooperating with officials of Internet-restricting countries in effecting the political censorship of online content." *Id.* § 101(2)–(3).

116. *See id.* §§ 101(2), 104(b)(6). As part of the bill, Congress also makes the following findings:

> Authoritarian foreign governments such as the Governments of Belarus, Cuba, Ethiopia, Iran, Laos, North Korea, the People's Republic of China, Tunisia, and Vietnam, among others, block, restrict, and monitor the information their citizens try to obtain. . . . Technology companies in the United States that operate in countries controlled by authoritarian foreign governments have a moral responsibility to comply with the principles of the Universal Declaration of Human Rights. . . . Technology companies in the United States have

Condoleezza Rice has already established the Office of Global Internet Freedom, which will oversee implementation of the Act and set policy.[117]

Under the Act, the President shall designate Internet-restrictive countries each year.[118] United States businesses cannot locate, within a designated Internet-restricting country, any electronic communication containing personally identifiable information, nor process or store such information by remote computing service facilities.[119] Further, the businesses cannot alter the operation of their search engines at the request of the foreign officials of any Internet-restricting country.[120] Information on communications with foreign officials, concerning censorship or terms to filter, must be turned over to the Office of Global Internet Freedom.[121] Any business that violates the provisions of this bill faces civil and criminal penalties.[122]

At present, few obstacles stand in the way of the Act's passage. The Act holds bipartisan support and numerous human rights organizations have endorsed its passage.[123] In particular, Amnesty International launched an official website with the purpose of supporting and promoting the Act.[124] Furthermore, the anticipated rise of China as an economic power, coupled with China's often antidemocratic policies, create the perfect political environment for anti-China legislation.[125]

> provided technology and training to authoritarian foreign governments which have been used by such governments in filtering and blocking information that promotes democracy and freedom.

Id. § 2(5), (11), (13).

117. *See* Press Release, United States Department of State, Secretary of State Establishes New Global Internet Freedom Task Force (Feb. 14, 2006), *available at* http://www.state.gov/r/pa/prs/ps/2006/61156.htm.

118. H.R. 275 § 105(a)(1)–(2). The Act provides no specific criteria in determining which countries qualify as Internet-restrictive.

119. *Id.* § 201.

120. *Id.* § 202(a).

121. *Id.* §§ 203, 204.

122. *Id.* § 206. Monetary penalties range between $10,000 to $2,000,000 depending on the extent of the violation, and criminal penalties include imprisonment of up to five years. *Id.*

123. As of January 27, 2008, four Republican and four Democratic congressmen have cosponsored the bill with Congressman Smith (R-NJ). Library of Congress, THOMAS, http://thomas.loc.gov/cgi-bin/bdquery/z?d110:H.R.275: (last visited Mar. 14, 2008).

124. *See* Irrepressible, http://irrepressible.info (last visited Mar. 14, 2008). Users may download briefings on Internet repression on China and join a campaign against general Internet repression.

125. American corporations outsource labor to China because they can pay Chinese workers less than American workers and do not need to abide by stringent American labor laws. However, this has caused a backlash in the United States and has created a negative sentiment towards China as more and more jobs disappear overseas. *See* Matt Richtel, *Outsourced All the Way*, N.Y. TIMES, June 21, 2005, at C1; Steven Greenhouse, *As Factory Jobs Disappear, Ohio Town Has Few Options*, N.Y. TIMES, Sept. 13, 2003, at A1.

Despite the Act's overwhelming support, some concerns remain: (1) whether this oversight by the United States State Department will cause Chinese citizens to distrust American corporations; (2) whether Congress should redefine the very way American corporations function abroad, that is, by forcing United States companies to move all Internet-related hardware out of Internet-restrictive countries; and (3) whether the United States should unilaterally set global Internet law.[126]

The first concern, whether Chinese citizens will distrust American corporations, arises from the Act's requirement that all communications by foreign officials discussing terms subject to filtering and censorship be delivered to the U.S. State Department.[127] In addition, even though United States companies must store personally identifiable information outside China, they nonetheless continue to have unlimited access to Chinese user information. Section 203 thus casts all American Internet companies operating in China as potential spies.

The Act also further strengthens the positions of Chinese companies. First, the Act cannot apply to Chinese companies because Chinese companies follow Chinese, not American, law. In fact, Chinese companies will comply with Chinese censorship law. Second, Chinese citizens do not lack technological alternatives. China's Baidu.com, another search engine, has a fifty-eight percent market share in China, compared to Google's twenty-three percent.[128] If Chinese users discover that American companies such as Google may disclose personal, private information to a foreign government, citizens will choose Chinese companies and censorship will prosper as such companies will fully comply with censorship laws.

The second critique of the Act focuses on the requirement that American companies not process or store personally identifiable information within Internet-restrictive countries, possibly resulting in the movement

126. To even address these concerns, we must first assume Chinese citizens will continue to use American search engines after the Act passes and the Chinese public becomes aware of its implications.

127. H.R. 275 § 203.

128. Loretta Chao, *China's Baidu, Sky High, Still Rates 'Buy': Even as Price, Competition Soar, Popular Web Site is an Analyst Favorite*, WALL ST. J., Aug. 8, 2007, at C3. American search engines are not the only companies with Chinese competitors: China's Huawei is the country's equivalent to Cisco Systems or Nortel Networks in Internet hardware production. In fact, Cisco sued Huawei for copyright infringement. Press Release, Cisco Systems Inc., Cisco Files Lawsuit Against Huawei Technologies (Jan. 23, 2003), *available at* http://newsroom.cisco.com/dlls/corp_012303.html.

of all Internet-related-hardware outside the borders of such countries.[129] This provision may alter the way the majority of American companies operate overseas in the affected countries, by forcing the companies to not house servers in those countries.

The greatest criticism of the Act questions whether the United States government should set Internet law worldwide. The Act runs straight into the black hole of international jurisdiction. No law dictates the enforcement of foreign judgments, much less resolves conflict between differing Internet regulations. By passing the Act, or an act with similar provisions, the United States draws first blood in this battle. Disregarding the barriers of sovereignty, the Act allows the United States to control businesses operating in another country. Closer to home, it is akin to a California state law applying in Nevada to Nevada citizens.

In addition, the drafters of the Act focused on the situation in China but neglected to examine the long-term global consequences of the Act. Even assuming the Act halts the censorship and persecution of dissident activists in China, with this precedent, European countries could pass equally intrusive laws aimed at the American subsidiaries of French companies. For example, as a result of precedent set by the Act, French law could force French companies operating in America to turn over information on all users who enter neo-Nazi search terms.

Aside from these criticisms, the Act also presents two pressing issues: (1) the plight of Chinese Internet users; and (2) the lack of international Internet regulations. In the absence of fruitful international action, the United States should take a leadership role and propel the discussion on resolving these problems. Perhaps the best way to initiate this discussion is by passing and enforcing an act that forces these issues upon the international community. Although unilateral action would certainly raise the importance of crafting lasting solutions to these issues, this action alone does not provide an immediate solution to a problem that affects Chinese citizens today. For that reason, independent of the passage of the Act, the United States should implement other short-term solutions.

B. No Public Regulation

Most simply, the United States can ignore China's use of American corporations to administer state-sponsored censorship and dispose of any

129. H.R. 275 § 201. In contrast to the Act, the Department of Justice and the FBI have contemplated rewriting United States wiretapping rules to require foreign ISPs to place within United States borders all servers used for United States customers. *See* Grant Gross, *FBI Floats Wide-Ranging Wiretap Proposal*, INFOWORLD, Sept. 14, 2006, http://www.infoworld.com/article/06/09/14/HNfbiwiretap_1.html.

plan of global Internet regulation. This choice to trust the Internet itself, market forces, or the judiciary to come up with the "right solution" is much less radical but much more complicated than it appears at first glance.

Even with China's stiff regulations, the mere presence of the Internet in China expanded free speech opportunities for Chinese citizens.[130] For example, message boards allow Chinese citizens to express their anger over their government's slow response to notify residents of harmful contaminants in their drinking water.[131] Further, as long as the ordinary citizen does not organize political protests, that citizen may chat, blog, and even conduct business with strangers.[132] Thus, even with the restrictions they face, as a result of the Internet's presence, Chinese citizens receive information from the outside world and communicate with each other more easily.

Moreover, the Chinese government lacks absolute control of information because the Great Firewall, while complex in nature, has sprung leaks. China does not employ citizens to surf the Internet and manually remove websites. Rather, China relies on intricate filtering technology as well as secrecy so that even Chinese companies must speculate as to which sites are banned.[133] The technologically sophisticated may code their way past the firewall—that is, until China's programmers counter by patching these holes. In addition, where the technology fails, information can bypass the censors.[134] Unfortunately, users cannot predict which websites pierce the firewall. However, relying on these leaks, supporters of nonregulation believe that although some content would be filtered, enough information would enter the country to enlighten the citizens and bring democracy.[135] Further, if a Chinese citizen accesses unfiltered

130. *See* discussion *supra* Part II.E.

131. In late 2005, benzene spilled into the Songhua river in China. The citizens of Harbin, a city in China, noticed the spill and the foul odor in their water supply, but the local papers and city officials professed ignorance of the situation. *See* Jim Yardley, *Spill in China Brings Danger, Cover-Up and Wild Rumors*, N.Y. TIMES, Nov. 26, 2005, at A1.

132. *See* Thompson, *supra* note 29, at 71, 155.

133. China can rely on "self-censorship" by companies because any misstep a company may make will result in legal penalties or infliction of physical punishment. *See supra* notes 89–100, 104–06, and accompanying text.

134. Some domain names are accessible while the URLs to those domains are blocked. *See supra* note 100.

135. For instance, former President Bill Clinton once stated in a speech on international relations, "We know how much the Internet has changed America, and we are already an open society. Imagine how it could change China. Now there's no

material before the firewall catches this material, nothing stops this citizen from distributing this material via cell phone or text message to other concerned citizens.[136]

In addition, modern day Chinese citizens appear aware but indifferent to their country's Internet censorship.[137] One scholar in China has noted that most users can work, travel, speak privately, and surf online with relative freedom, so that censorship itself does not disrupt daily life.[138] Citizens interviewed by the *New York Times* after the Google firewall incident professed knowledge of the censorship but adopted a long-term perspective, believing the government would ultimately fail in censoring the Internet.[139] Another Chinese citizen shared the belief of early scholars worldwide that the Internet by itself plants the seeds for democracy in Chinese youth.[140] For the ordinary Chinese citizen, Internet censorship may not be so bothersome, as compared to the burdens of everyday life, to inspire activism.[141]

Although opting for no regulation is an easy and tempting path to take, unfortunately China has neither relented nor shown signs of relenting in its quest to restrict Internet access. China's attempt at Internet regulation cannot be compared to the failed attempts of France and Germany. In fact, as evidenced by the fate of Shi Tao, China's firewall has proven more sophisticated, its police force more brutal, and its rules more stringent than ever anticipated. Beyond the lives at stake lies the possibility that China will completely control its Internet one day, blocking all outside access from its citizens. As a result, the Internet cannot be entrusted to bring democracy to China on its own.

The Internet has also failed to bring democracy to China through market forces. Google chose to stay in China and comply with its censorship laws to maintain a foothold in an immense potential market. This is a choice echoed by non-Internet companies: to outsource

---

question China has been trying to crack down on the Internet—good luck. . . . That's sort of like trying to nail Jello to the wall." Bill Clinton, Address at the Paul H. Nitze School for Advanced International Studies at John Hopkins University (March 8, 2000) (transcript available at http://canberra.usembassy.gov/hyper/2000/0308/epf302.htm).

136. Chinese citizens are increasingly using cell phone text messaging as a way of passing information quickly, organizing protests, and bypassing censors. *See* Jim Yardley, *A Hundred Cellphones Bloom, And Chinese Take to the Streets*, N.Y. TIMES, Apr. 25, 2005, at A1.

137. The PBS documentary series *Frontline* has explored China's censorship of its political activists on the Internet and in print media. This particular episode contains extensive interviews comparing Western views of China's censorship with opinions by Chinese scholars. *Frontline: The Tankman* (PBS television broadcast Apr. 11, 2006) (transcript available at http://www.pbs.org/wgbh/pages/frontline/tankman).

138. Li, *supra* note 89, at 37.

139. *See* Thompson, *supra* note 29, at 156.

140. *Id.* at 66, 156.

141. *Id.* at 156.

manufacturing and service-oriented labor to China in the name of profit and the promotion of shareholder value. As the largest potential customer base in the world, market forces direct companies toward China, and China requires the companies to comply with its laws.[142]

Finally, if the United States government does not regulate the Internet, the judiciary may develop common law to address the different situations. However, as Justice Benjamin Cardozo so aptly put it:

> We are not so provincial as to say that every solution of a problem is wrong because we deal with it otherwise at home. The courts are not free to refuse to enforce a foreign right at the pleasure of the judges, to suit the individual notion of expediency or fairness. They do not close their doors, unless help would violate some fundamental principle of justice, some prevalent conception of good morals, some deep-rooted tradition of the common weal.[143]

A court will not apply foreign law if it violates a fundamental principle of domestic public policy.[144] In the United States, these fundamental principles correspond to the values articulated in our Puritanical roots. In other countries, these fundamental principles reflect different values accorded by each culture. As a result, even if the judiciary develops common law to address corporate responsibility for Internet censorship abroad, other countries need to apply these laws.[145] This solution also runs into old issues of United States imperialism and reopens grudges between the Old World, New World, and developing countries.

C. Corporate Accountability

Responsibility for Internet regulation in China starts with the offending corporations themselves. Those persons or entities that hold an American corporation accountable can direct the corporation to change its policies in China. Accountability exists when an agent is held to answer for

142. In 2005, China held the top spot in the Foreign Direct Investment (FDI) Confidence Index for the third year in a row. GLOBAL BUSINESS POLICY COUNCIL, FDI CONFIDENCE INDEX (2005), http://www.atkearney.com/shared_res/pdf/FDICI_2005.pdf. The FDI measures long-term investments by a foreign entity into another country's economy. It represents investor confidence in the economy of any given country. In the FDI index, India and the United States held second and third place, respectively. *Id.* at 1–2.

143. Loucks v. Standard Oil Co., 120 N.E. 198, 201–02 (N.Y. 1918).

144. Anne-Marie Slaughter, *Disaggregated Sovereignty*, *in* GLOBAL GOVERNANCE AND PUBLIC ACCOUNTABILITY 35, 53–54 (David Held and Mathias Koenig-Archibugi eds., 2005).

145. *See id.* (discussing the "principle of legitimate differences").

performance that involves some delegation of authority to act.[146] In that sense, a corporation's owners, its institutional and individual shareholders, can direct corporate policy because owners are principals and officers are agents of the corporation. But corporations in the United States must also answer to those to whom they are indebted, such as their creditors and customers. Finally, corporations are internally accountable to their employees and externally accountable to any business entities with which they have a working relationship, such as distributors and suppliers.[147] One of the primary goals of a corporation is to increase shareholder wealth by raising the price of the company's stock so that any actions with a deleterious effect on the current or projected stock price of a company will motivate the company to take action.

Shareholders may hold a corporation accountable for its actions by taking action to deter the corporation from engaging in the discouraged activity. Most recently, as a result of Enron, Worldcom, and other scandals involving elaborately falsified financial statements, shareholders demanded, and Congress responded by imposing new regulations on all public companies.[148] In addition, institutional shareholders may use their substantial voting power and leverage over a company's share price to influence the board of directors of an offending corporation.[149] Although individual

146. Mathias Koenig-Archibugi, *Transnational Corporations and Public Accountability*, *in* GLOBAL GOVERNANCE AND PUBLIC ACCOUNTABILITY, *supra* note 144, at 110, 112.

147. *See id.* at 113–14.

148. In 2001, American energy giant Enron revealed that it had sustained its profits as a result of massive internal accounting fraud. Enron subsequently filed the second largest United States claim for bankruptcy in history. Richard A. Oppel, Jr., & Andrew Ross Sorkin, *Enron Corp. Files Largest U.S. Claim for Bankruptcy*, N.Y. TIMES, Dec. 3, 2001, at A1. Thousands of employees lost not only their jobs but also their savings in the now worthless Enron stock. *See* Kate Murphy, *Enron's Collapse: The Employees Sent Home To Sit and Wait By the Phone*, N.Y. TIMES, Dec. 4, 2001, at C9. The ensuing investigation pointed fingers straight at Enron's auditors. *See* Alex Berenson, *Enron's Collapse: Watching The Firms That Watch The Books*, N.Y. TIMES, Dec. 5, 2001, at C1. After the American telecommunications company Worldcom revealed that it also engaged in deceptive accounting practices and then declared the largest United States claim for bankruptcy in history, Congress passed the Sarbanes-Oxley Act to promote corporate governance and accountability. Simon Romero & Riva D. Atlas, *Worldcom Files for Bankruptcy; Largest U.S. Case*, N.Y. TIMES, July 22, 2002, at A1; *see* Jeffrey N. Gordon, *Governance Failures of the Enron Board and the New Information Order of Sarbanes-Oxley* 3–5, 10–16 (Columbia Law Sch. Ctr. for Legal and Econ. Studies, Working Paper No. 216, 2003), *available at* http://ssrn.com/abstract=391363 (discussing implications of Sarbanes-Oxley on future Enron-like situations).

149. California's public pension fund, CalPERS, has "long sought ways to use the power of its holdings to influence corporate behavior. Its trustees have argued that doing so is a crucial part of their fiduciary duty, because insisting on good corporate governance is likely to bring about more valuable shares." Mary Williams Walsh, *Calpers Ouster Puts Focus On How Funds Wield Power*, N.Y. TIMES, Dec. 2, 2004, at C10. In the 2004 election, however, CalPERS's Democratic trustees came under attack by Republicans, who claimed CalPERS puts social responsibility ahead of shareholder value. *Id.*

shareholders have little clout as compared to institutional investors, these shareholders can destroy a company's reputation in the media.[150] In addition, individual shareholders may punish corporations through the judicial system in shareholder lawsuits.[151] Finally, the individual shareholders can simply sell off their holdings.

Thus, the power to change the policies of these Internet companies lies in the hands of their shareholders and business partners. To date, this has not occurred—the stakeholders seem content with the direction these companies have chosen.[152] Not surprisingly, shareholders enjoy having a foothold in an immense potential economic market.[153]

---

150. Corporations are finding it increasingly difficult to hide labor violations in foreign countries from the American public. *See* Cynthia A. Williams, *Corporate Social Responsibility in an Era of Economic Globalization*, 35 U.C. DAVIS L. REV. 705, 736–37 (2002).

151. Several law review articles explore the possibility of shareholders holding corporations responsible for human rights violations under the Alien Tort Claims Act (ATCA). *See* Francisco Rivera, *A Response to the Corporate Campaign Against the Alien Tort Claims Act*, 14 IND. INT'L & COMP. L. REV. 251, 276–77 (2003) (acknowledging weaknesses to the ATCA approach but chastising corporations for attacking the ATCA when no other better remedy exists and when corporations themselves do not engage in corporate responsibilities); Saman Zia-Zarifi, *Suing Multinational Corporations in the U.S. for Violating International Law*, 4 UCLA J. INT'L L. & FOREIGN AFF. 81, 104–14 (1999) (applying the ATCA and justifying its use against corporations engaged in human rights abuses); Beth Van Schaack, *With All Deliberate Speed: Civil Human Rights Litigation as a Tool For Social Change*, 57 VAND. L. REV. 2305, 2345–47 (2004) (cautioning against potential backlash in ATCA lawsuits that may result in a focus on litigation at the cost of forgetting the victims).

152. The tide may slowly be turning. Institutional shareholder Boston Common Asset Management recently introduced a shareholder resolution requiring Cisco Systems to specify the steps taken by the company to reduce the likelihood that its practices in China may enable or encourage the violation of human rights. *See* Press Release, Boston Common Asset Management, LLC, Human Rights and Internet Fragmentation Proposal Receives Record Shareholder Support (Nov. 15, 2006), *available at* http://www.bostoncommonasset.com/news/cisco-agm-111506.html. The resolution failed, but twenty-nine percent of Cisco's shareholders voted in its favor, up from eleven percent the year before when the investment firm introduced the same resolution. *Id.* The shareholders voted for the resolution despite vehement opposition by Cisco's board, which includes Jerry Yang, the president of Yahoo!. Press Release, Reporters Without Borders, Shareholders Ask Cisco Systems to Account for its Activities in Repressive Countries (Nov. 17, 2006), *available at* http://www.rsf.org/article. php3?id_article=19782. In addition, the New York City Pension Fund has targeted the shareholders of Google, Yahoo!, and Microsoft with similar resolutions. The city's pension fund has considerable financial clout, owning nearly 400 million dollars worth of stock in the two companies. The Yahoo! resolution received more than 15% of shareholder votes, with the Google and Microsoft resolutions receiving 3.8% and 3.9% respectively. Press Release, William C. Thompson, Jr., N.Y. City Comptroller, Thompson Pressures Yahoo! and Google to Establish Policies Against Censorship (Jan. 31, 2008), *available at* http://www.comptroller.nyc.gov/press/

Despite the reluctance of institutional shareholders to promote the advancement of human rights, the general public can also hold corporations accountable for their actions.[154] Because corporations touch so many facets of society and because of their visibility in the public in general, society has often called upon corporations to redefine the status quo. For example, public groups have petitioned corporations to protect workers' rights, conform to environmental safety standards, and promote the advancement of women and minorities in the workplace.[155] Watchdog organizations can also harm a company's reputation and, in some cases, affect that company's practices overseas.[156]

If Chinese and American corporations refuse to act to change the status quo, the American and Chinese public may force these corporations to take responsibility for their actions.[157] Already, news of Internet censorship in the United States caused the legislature to initiate the

---

2008_releases/pr08-01-009.shtm. In January 2008, New York City Comptroller William C. Thompson Jr. resubmitted the Yahoo! and Google resolutions on behalf of the fund. *Id.*

153. Shareholder sentiment with regard to a specific element of corporate philosophy may be difficult to quantify. Just as a citizen will vote for the election candidate that best represents that citizen's views, a shareholder will not oust the board of directors if he or she disagrees with a part but not all of the of board's philosophies.

154. Koenig-Archibugi, *supra* note 146, at 112.

155. Williams, *supra* note 150, at 736–40 (noting that after a negative publicity campaign aimed at Nike's labor practices, Nike has since become the picture of social responsibility); *see also* Danny Hakim, *Bicoastal Blues For G.M. and Ford*, N.Y. TIMES, Apr. 23, 2005, at C1 ("[T]he electoral party of [the ten states adopting California's car emission standards] . . . puts considerable pressure on automakers to develop more fuel-efficient vehicles.").

156. Even if an organization makes a wholly ridiculous claim against a corporation, each accusation slowly erodes the company's goodwill and adversely affects its stock prices. Corporations may heed shareholders' concerns over a decreasing or stagnant stock price because the directive of a corporation is to increase shareholder value. For example, constant criticism over Wal-Mart's alleged choice of profits at the cost of exploiting low-income workers has resulted in a stagnant stock price in recent years, despite steadily increasing sales and profits. As a result, Wal-Mart now must examine its corporate image. *See* Liza Featherstone, *Wal-Mart's P.R. War*, SALON, Aug. 2, 2005, http://dir.salon.com/story/news/feature/2005/08/02/walmart/index.html?pn=1 (distinguishing the anti-Wal-Mart movement from other public outcries for corporate responsibilities, in part because activists equate fighting Wal-Mart with opposing the current President and also because of the willingness of the activists to engage politicians and pass legislation against Wal-Mart); WAL-MART STORES INC., 2005 ANNUAL REPORT 15 (2005) (noting frustration on the part of Rob Walton, Chairman of the Board of Directors: "It is frustrating that over the last five years, our sales have gone up almost 83 percent, and our earnings have grown almost 100 percent, but our stock price hasn't moved.").

157. Some publicly-traded Chinese companies are actually partially owned by the state. For example, the Chinese government partially owns Baidu and Sina.net. Consequently, if these companies succeed to Google's share of the Chinese market, effective shareholder oversight may be impossible to obtain.

Global Online Freedom Act.[158] The media and public interest groups such as Amnesty International now broadcast what they perceive to be the wrongs of these companies on national news and on the front of pages of prominent newspapers.[159] This erosion of the reputation of these companies and the call for accountability overseas by public interest groups and by the media has begun. And if such erosion depresses the stock prices of these companies, it will not be forgotten. Google's loud proclamations of philanthropy and its do-no-evil motto make it a particularly vulnerable target.[160] Although the Google Foundation funds research into environmentally friendly hybrid car engines, promotes literacy, and fights poverty, it does nothing to aid the human rights situation in China despite the situation's close ties to Google's overseas operations.[161] As a result, public groups should focus on Google's ability to remedy the human rights situation in China.

D. Proxy-Blocking Identity-Concealing Technology

The 2003 version of the Global Internet Freedom Act included a promising proposal: the use of government-funded, proxy-blocking

158. Another possible, but highly theoretical, solution that Congress could employ is to set the penalties associated with violating the Act at a level high enough to significantly harm the company's profits in China, but not so high as to deter the company from exiting the market completely. The penalties must be set so that shareholders would still profit, albeit very slightly, from their investment in the offending company. As a result, the shareholder would not have an incentive to pressure the company to withdraw because the shareholder would still benefit more financially from the company's presence in China than its absence and would instead pressure China to change. A somewhat relevant example would be the European Union's imposition of a $600 million fine on Microsoft for breach of European antitrust regulations. Microsoft had ample knowledge of the antitrust regulations, but the size of the market convinced Microsoft to breach these regulations. Unlike the China situation, though, Microsoft's shareholders allowed Microsoft to remain in Europe. The idea behind the fines in the Act would be to set recurring fines at a level that would force action. *See* Paul Meller, *Microsoft Pays Fine Imposed by Europe*, N.Y. TIMES, July 1, 2004, at C7.

159. Many of the *New York Times* articles cited by this Comment appeared on the front page. In particular, Clive Thompson's piece, *Google's China Problem (and China's Google Problem)*, appeared on the front cover of the *New York Times Magazine* on April 23, 2006. *See generally* source cited *infra* note 160; Thompson, *supra* note 29.

160. Google created the for-profit philanthropist group, the Google Foundation, with $1 billion of seed money. Katie Hafner, *Philanthropy Google's Way: Not the Usual*, N.Y. TIMES, Sept. 14, 2006, at A1.

161. *See* Google.org Homepage, http://google.org/ (last visited Mar. 14, 2008).

technology to tunnel past China's censors.[162] In the United States, proxy-blocking technology appeals to those users who wish to hide personal information and conceal their Internet history as they navigate through different websites. However, this technology can also circumvent censors. It works as a middleman; instead of connecting directly to a website, the middleman will take a user's order and connect to the site under the middleman's name.[163] In this way, the visited site registers the middleman's identity and location, and the actual user remains largely anonymous. Those monitoring the activities of the user will only see connections going to and from the middleman. The use of government funds to promote proxy-blocking software in Internet-restrictive countries occurred in Iran.[164] There the United States enlisted Anonymizer, a company specializing in Internet privacy technology, to promote free speech and to protect Iranian Internet users from government censorship.[165]

In March 2006, Anonymizer announced it would take its technology to China to help Chinese citizens circumvent the Chinese firewall.[166] In China, Anonymizer faces two main problems. The first poses a conundrum: how to spread word of a product to circumvent censors when the government censors news of that product. Anonymizer and other similar services rely on word of mouth within the Chinese community to solve this problem. The technologically savvy and dedicated online bloggers do not need commercial products to circumvent the firewall. Private proxy servers perform the same function as Anonymizer.[167] Ideally, these technologically savvy users would receive notice about other

162. This proposal did not make it into the 2006 or 2007 versions of the Act. *Compare* H.R. 48, 108th Cong. (2003), *with* H.R. 4780, 109th Cong. (2006), and H.R. 275, 110th Cong. (2007).

163. The middleman's name is actually the middleman server's IP address. Justin Boyan originally developed Anonymizer, a proxy-blocking service, in 1995. He explains the history of Anonymizer, how it works, and its flaws on his website, The Anonymizer, http://www.december.com/cmc/mag/1997/sep/boyan.html.

164. Hiawatha Bray, *Beating Censorship on the Internet: Tools Mask User IDs, Give Alternative Routes to Sites*, BOSTON GLOBE, Feb. 20, 2006, at A10.

165. The Anonymizer, *supra* note 163; Bray, *supra* note 164.

166. Press Release, Anonymizer, Chinese Citizens Get Censor-Free Internet Through Anonymizer (Mar. 31, 2006), *available at* http://www.anonymizer.com/consumer/media/press_releases/03312006.html. Anonymizer previously worked with Voice of America to develop similar technology for use in China. *See* Press Release, Anonymizer, Anonymizer to Provide Censor-Free Internet to China (Feb. 1, 2006), *available at* http://www.anonymizer.com/consumer/media/ press_releases/02012006.html.

167. A computer in a foreign country may be set up to act as a server, performing the same function as Anonymizer in blocking a user's identity. However, not all Chinese citizens have access to private computers set up in foreign countries.

commercial proxy-blocking services during their uncensored surfing and spread word to the Chinese community.[168]

The active intervention of the Chinese government presents Anonymizer's second problem. Once the government encounters a proxy-blocking site, that site is shut down. Anonymizer, however, solves this issue by maintaining a list of users and informing users each time the website hosting the technology changes.[169] Ironically, China's trust in its self-maintaining firewall also aids Anonymizer, because China does not employ people to search the Internet to manually remove offending sites. Consequently, the hosting website need not change too frequently, but only when caught by this firewall.

Although programs such as Anonymizer provide an efficient and effective short-term solution to eluding China's filters, these programs may conflict with current American security concerns. Zero Knowledge, an early rival to Anonymizer, shut its doors roughly a month after the terrorist attacks of September 11, 2001.[170] Safeweb, another rival partially funded by the U.S. Central Intelligence Agency, shut down its free site shortly thereafter.[171] Although Zero Knowledge attributed its decision to poor business, both sites had come under heavy criticism in the days after the attacks for their potential ability to aid and abet terrorists in communicating with each other anonymously.[172]

Historically, anonymous speech played a vital role in the founding of this country.[173] In more recent times, the Supreme Court has upheld the

168. Word can be spread either verbally, online, or via cell phone.

169. When Anonymizer for Chinese citizens was first released in March 2006, it was located at http://www.xifuchun.com/. However, this site no longer exists. Only Chinese users of this service know its current URL. *See* Press Release, Anonymizer (Feb. 1, 2006), *supra* note 166.

170. Julie Hilden, *The Death of Anonymous Speech on the Internet? How September 11 May Alter Our First Amendment Rights Online*, FINDLAW, Nov. 29, 2001, http://writ.news.findlaw.com/hilden/20011129.html.

171. *Id.* Safeweb has since been bought out by Symantec, and has discontinued its services. *See* Safeweb, http://www.safeweb.com (last visited Mar. 14, 2008) (transferring searches to the Symantec site).

172. *See* Hilden, *supra* note 170.

173. In the days preceding the American Revolution, political activists published their views anonymously to avoid British retribution. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) ("Anonymity is a shield from the tyranny of the majority."); *see also id.* at 360 (Thomas, J., concurring) ("There is little doubt that the Framers engaged in anonymous political writing."). Similarly, Alexander Hamilton, John Jay, and James Madison published the *Federalist Papers* under the pseudonym Publius. *See* Talley v. California, 362 U.S. 60, 65 ("Even the Federalist Papers, written in favor of our Constitution, were published under fictitious names."). Even today,

right of religious and political activists to express their views anonymously.[174] However, as a result of the terrorist attacks on September 11, 2001, and the revelation that the terrorists communicated with each other online, anonymity on the Internet has begun to erode.[175]

Investigations of terrorist organizations after the attacks on September 11 revealed the extent of terrorist dependence on the Internet. Terrorist groups such as Al-Qaeda use the Internet for recruitment and promotion of their activities.[176] These groups release videos of their exploits as well as training materials for would-be terrorists online.[177] In addition, terrorists communicate with each other in Internet chat rooms.[178]

In the interest of protecting national security, President Bush granted greater power to law enforcement officials. Five years after the attacks, many of these actions still curtail the range of anonymous speech on the Internet. For example, the renewal of the Patriot Act in 2005 also extended the life of a provision that gave government agencies expanded surveillance powers.[179] More famously, President Bush allegedly issued an executive order authorizing the National Security Agency (NSA) to eavesdrop on Americans inside the United States.[180] This warrantless

---

politicians and their staff members regularly communicate anonymously with the press. Anonymous speech in politics is often necessary to preserve one's public image. *See* Mark Leibovich, *Foley Case Upsets Tough Balance of Capitol Hill's Gay Republicans*, N.Y. TIMES, Oct. 8, 2006, at A1 ("[M]any gay Republicans interviewed for this article . . . would speak only anonymously for fear of adversely affecting their career.").

174. *See* Watchtower Bible & Tract Soc'y of New York, Inc. v. Village of Stratton, 536 U.S. 150, 151–52 (2002) (holding an ordinance, requiring solicitors and canvassers to obtain and display a permit prior to engaging in door-to-door solicitation, to be in violation of the First Amendment); *see also McIntyre*, 514 U.S. at 357 (weighing the value of free speech against its misuse in political campaigning and holding that the state cannot bar all anonymous election-related pamphleting).

175. *See* Jennifer B. Wieland, Note, *Death of Publius: Toward a World Without Anonymous Speech*, 17 J.L. & POL. 589, 625–27 (2001) (noting that ISPs have agreed to work with the government in an unspecified manner and that the FBI will now employ technology to read encrypted Internet messages of suspected terrorists).

176. Hilden, *supra* note 170; Robert F. Worth, *Jihadists Take Stand on Web, and Some Say It's Defensive*, N.Y. TIMES, Mar. 13, 2005, at A22.

177. Hilden, *supra* note 170.

178. *See* Worth, *supra* note 176.

179. The Patriot Act amended the Foreign Intelligence Surveillance Act of 1978 (FISA). *See* Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1805 (2000); Sheryl Gay Stolberg, *Senate Passes Legislation To Renew Patriot Act*, N.Y. TIMES, Mar. 3, 2006, at A14. On September 28, 2006, the House of Representatives passed a bill that would "update" the Foreign Intelligence Surveillance Act (FISA). Electronic Surveillance Modernization Act, H.R. 5825, 109th Cong. (as passed by House, Sep. 28, 2006).

180. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1. However, the Bush Administration insists that this news report is grossly inaccurate. The investigation continues into whether the President issued this executive order. The Electronic Privacy Information Center (EPIC), a public policy group dedicated to protecting privacy and freedom of speech on the Internet, has filed a lawsuit against the Department of Justice seeking documents relating to the order

eavesdropping included reading the emails of any citizen linked, even indirectly, to suspected terrorists.[181]

Despite the threat to national security, the United States government should not condemn the use of proxy-blocking services to aid Chinese citizens in defeating censorship because proxy-blocking services appear to be the best solution at this time. Many Chinese Internet users already utilize this service to shield their identities. Further, Anonymizer allows citizens to exercise free speech online absent fear of potential persecution from their government. Because this promotion of online anonymous speech may harm America's national security, the United States government is unlikely to fund this enterprise. Even if this service goes against current United States domestic policy, this country cannot forget its historical roots in anonymous speech, its worldwide place as the champion of free speech, and the human lives at stake in China absent this solution. Funding or not condemning the use of proxy-blocking technology in China would be the best short-term solution.

E. International Internet Control

In 1999, the Hague Conference on Private International Law adopted the preliminary draft of a treaty that would enforce judgments across international borders. Notably, the treaty would include Internet regulations.[182] However, despite fourteen years of negotiations, the treaty remains unfinished with no end in sight.[183] Even if the treaty materializes, member states may not endorse it without extensive objections, if at all. In 2005, the Hague Conference finished the Convention on Choice of Court Agreements. This scaled-down treaty, which excludes common Internet issues such as copyright and intellectual property issues, languishes unsigned by any member state.[184]

---

of NSA surveillance. The complaint can be found on EPIC's website at http://www.epic.org/privacy/nsa/complaint_doj.pdf (last visited Mar. 14, 2008).

181. Risen & Lichtblau, *supra* note 180, at A16.

182. Proposed Hague Conference Convention on Jurisdiction and the Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters, http://www.cptech.org/ecom/jurisdiction/hague.html (last visited Mar. 14, 2008) (preliminary drafts and meeting minutes).

183. *See id.*

184. Convention on Choice of Court Agreements, June 30, 2005, 44 I.L.M. 1294, *available at* http://www.hcch.net/index_en.php? act=conventions.text&cid=98. Under this treaty, signatories agree to recognize and enforce judicial decisions reached by other signatory states. *Id.*

Fortunately, a treaty may not be necessary in this realm because the Internet Corporations for Assigned Names and Numbers (ICANN) already functions as an international treaty organization.[185] ICANN is the nonprofit entity in charge of assigning and managing domain names and IP addresses, a function vital to the survival and organization of the Internet.[186] The ICANN concept emerged during the Clinton Administration in response to the growing privatization of the Internet and the fear that national governments would impose upon the global arena of the Internet inconsistent or conflicting national laws.[187] As a result of its birth in the United States, ICANN operates under a contract with the Department of Commerce from ICANN's headquarters in California.[188] All potential conflicts fall under California state law and the United States government theoretically has the final word over ICANN's actions.[189] However, the United States has never acted on this authority.[190] The international community perceives this conflict of interest—the mere possibility that one country could control the Internet—as particularly unsettling.[191]

However, ICANN's position as the incumbent international Internet regulatory agency may yet be salvageable. Professor Jonathan Weinberg aptly notes that ICANN functions in many ways like an administrative agency with a single exception.[192] Unlike administrative agencies,

185. The remarkable thing about ICANN is that it is an international body set to solve international issues, but was created absent a treaty or international negotiation. Milton Mueller, Dancing the Quango: ICANN and the Privatization of International Governance 6 (Feb. 11, 2002), *available at* http://ischool.syr.edu/~mueller/quango.pdf.

186. *Id.* at 1.

187. *Id.* at 3. Ironically, the Act would impose laws that conflict with Chinese laws.

188. *See* Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 2032–33 (2006). For other private alternatives to ICANN, see Michael Froomkin, *Habermas@Discourse.net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749, 798–817 (2003). To date, ICANN still operates from California. In fact, ICANN held its last meeting in "its home town of Los Angeles." 30th International Public ICANN Meeting, http://losangeles2007.icann.org/ (last visited Mar. 14, 2008).

189. "Externally, ICANN is an organisation incorporated under the law of the State of California in the United States. That means ICANN must abide by the laws of the United States and can be called to account by the judicial system i.e. ICANN can be taken to court." About ICANN, http://losangeles2007.icann.org/icann (last visited Mar. 14, 2008).

190. Victoria Shannon, *Other Nations Hope to Loosen U.S. Grip on Internet*, N.Y. TIMES, Nov. 15, 2005, at C14.

191. *Id.* In contrast, opponents of international control point to the supporters of this proposal: the Internet-restrictive countries of China, Iran, and Syria, along with the European Union and its member states. *Id.*

192. For example, ICANN appoints its own board of directors, which is not accountable to the international community or general American public. *See* Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187, 235–36 (2000). ICANN has no need to reach a consensus on its decisions and, in fact, will choose to exclude the views of those who do not come from technological backgrounds. *Id.* at 249

ICANN's decisions are not subject to review by any independent body other than ICANN itself.[193] This only furthers criticism over the opaqueness of ICANN's decisions and fuels the international fear that the United States controls the Internet because ICANN is based in the United States.

Professor Weinberg does not suggest judicial review of ICANN's decisions but instead advises ICANN to gain legitimacy through its substantive decisions and to decide technological questions while refraining from setting policy.[194] Although wholly plausible, this suggestion seems to entrust ICANN with the duty of building its own reputation in the international community, when much of that community has already formed its opinion against ICANN.[195] As Weinberg observes, ICANN needs legitimacy and acceptance to accomplish its goals because ICANN rests on a precarious perch and cannot afford to antagonize its sponsoring government, important Internet companies, and sources of funding.[196] It would be in ICANN's interest to actively seek some type of independent review of its rulings outside the United States to provide the international community with at least the illusion of fairness and to distance itself from the United States. By establishing itself as a legitimate international Internet regulatory agency, ICANN can assist in solving the Chinese Google problem.

(noting ICANN excludes "people with no understanding of ICANN"). According to Weinberg, ICANN also sets policy and creates legal relationships. *See id.* at 223–24. ICANN argues that it does not set policy, but performs a highly technological function—the regulation of domain names. Yet, Weinberg counters, the very issues of trademark dispute resolution and cybersquatting are at heart issues of policy that concern technology and are not purely technological questions. *Id.* at 223. In addition, to endorse its own legitimacy, ICANN has adopted three techniques of administrative agencies: it publicized the techniques it follows in making policy rulings, developed a formal procedure for review of the rulings, and adopted requirements of standing, timeliness, and exhaustion with regard to the reviews of its rulings. *Id.* at 224. However, ICANN cannot transform itself into an administrative agency because it still does not answer to the United States government. *Id.* at 225–29.

193. *Id.* at 231–35. Weinberg also notes that no ICANN institution exists to perform the function that judicial review performs for administrative agencies. *Id.* at 233.

194. *See id.* at 259–60.

195. *See* Jennifer L. Schenker, *Nations Chafe at U.S. Influence Over the Internet*, N.Y. TIMES, Dec. 8, 2003, at C1.

196. Weinberg, *supra* note 192, at 255–56. "ICANN is the product of a somewhat precarious bargain between the Internet technical hierarchy, a few major e-commerce and telecommunications firms, the intellectual property interests . . . the European Union, the US Department of Commerce, and one or two other national governments, notably Australia." Mueller, *supra* note 185, at 7.

The United States and the international community itself fail to aid ICANN in this endeavor. In September 2006, the United States Department of Commerce renewed its three-year contract with ICANN.[197] In exchange, the United Nations created an Internet Governance Forum, aimed at developing international Internet policy.[198] Despite being a promising step in the creation of an international body, the majority of Internet corporations are based in the United States, which is a direct result of the Internet originating in the United States.[199] Although the United States's invention of the Internet does not grant the United States property rights over the Internet, it does mean that efforts toward moving the Internet under international control are likely to be stalled by the United States and its army of Internet corporations.[200]

F. China and the World Trade Organization

On December 11, 2001, China committed itself to the international community when it became the one hundred and forty-third member of the World Trade Organization (WTO).[201] In reaching this point, China agreed to all WTO agreements, including the provisions requiring application of Most Favored Nation (MFN) treatment.[202] Commentators

197. Joint Project Agreement Between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers (Sept. 29, 2006), http://www.icann.org/general/JPA-29sep06.pdf. This move undermines the international community's belief that ICANN acts independently. Victoria Shannon, *U.S. Loosens Its Control Over Web Address Manager*, N.Y. TIMES, Sept. 30, 2006, at C4.

198. The Internet Governance Forum (IGF), http://www.intgovforum.org (last visited Mar. 14, 2008) (providing IGF's policy and current projects). The 2006 meeting of the Internet Governance Forum focused on the use of non-Latin characters in domain names. Some countries, China included, see the sole use of Latin characters in domain names as an attack upon their culture. Victoria Shannon, *A Web Conflict Centers On Languages Used in Addresses*, N.Y. TIMES, Oct. 30, 2006, at C9.

199. Internet corporations refer to companies primarily engaged in Internet infrastructure and content development.

200. The fact that the United States invented the Internet is not as important as the fact that the vast number of Internet hardware and service corporations still remain in the United States. The lobbying power of these corporations will make it difficult to implement policy against their best wishes. Conversely, though, with the majority of Internet corporations headquartered in the United States, this country is in a unique position to spearhead international Internet policy. However, this suggestion would not be taken well within the international community.

201. Jeffrey L. Gertler, *China's WTO Accession—The Final Countdown*, *in* CHINA AND THE WORLD TRADING SYSTEM 55, 61 (Deborah Z. Cass et al. eds., 2003).

202. Most favored nation (MFN) status accords the receiving country equal treatment with any other country in the WTO. *Id.* The United States granted China MFN status but can remove this status to punish China for its human rights violation, thus placing China at a trade disadvantage relative to other countries that trade with the United States. Unfortunately, the offending corporations as well as all other American corporations profiting in China will lobby against this proposal. *See* Tom Zeller, Jr., *Web Firms Questioned On Dealings In China*, N.Y. TIMES, Feb. 16, 2006, at C1.

noted China's new willingness to reduce its tariff and nontariff barriers and to allow foreign competition within its borders.[203] More importantly, China is now bound by the rules of the WTO and must resolve its trade disputes under international law.[204] It is possible that over time the global marketplace and the WTO will force China to accept and follow international law.

Moreover, the pressure of the international economic community, as opposed to the international community as a whole (such as that embodied in the United Nations), has already prevailed against China's attempt to create its own closed wireless Internet standard. In 2003, China required all Wi-Fi devices within its borders to incorporate WLAN Authentication and Privacy Infrastructure (WAPI) technology.[205] WAPI forces every user of a wireless network to register with a centralized authentication point.[206] However, under pressure from the WTO, China ultimately suspended this attempt to create and control the underlying standards governing Internet access.[207]

IV. RECOMMENDATION

Some experts believe the issue is still unripe for meaningful discussion, and that when the time does arrive to take action, only a

203. *See generally id.*; *see also* Shi Guangsheng, *Introduction: Working Together for a Brighter Future Based on Mutual Benefit*, *in* CHINA'S PARTICIPATION IN THE WTO 15, 15–21 (Henry Gao & Donald Lewis eds., 2005).

204. Qingjiang Kong, *Enforcement of WTO Agreements in China: Illusion or Reality?*, *in* CHINA AND THE WORLD TRADING SYSTEM, *supra* note 201, at 132. However, if China violates the WTO agreements it is entirely possible that China will not submit to the WTO's dispute resolution system. This is on account of South Korea's and Japan's particularly negative experiences with the same system. For an explanation of their experience, see Henry Gao, *Aggressive Legalism: The East Asian Experience and Lessons for China*, *in* CHINA'S PARTICIPATION IN THE WTO, *supra* note 203, at 315, 322–34.

205. GOLDSMITH & WU, *supra* note 98, at 101.

206. *Id.*

207. *Id.* at 102. The authors also aptly note that while China may attempt to control the Internet by controlling the standards guarding access and use, other offenders attempt to exercise control in different formats on different topics. As discussed before, ICANN holds tightly to its jurisdiction over domain name registration from its base in the United States. In Europe, regulators applied the continent's broad privacy laws to the Microsoft Internet service's collection of user data. These laws forced Microsoft to implement global changes to its service. *Id.* at 174–77; *see* Article 29 Data Protection Working Party, *Working Document on On-line Authentication Services* 4–11 (Jan. 29, 2003), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_en.pdf.

globally directed and implemented solution will suffice.[208] The future long-term solution may consider cultural perceptions of the Internet, redefining geographic and political borders, and possibly rewriting the underlying structure of the Internet itself.[209]

However, this Comment only addresses the short-term solution to China's censorship of the Internet and subsequent persecution of its citizens. This Comment also suggests a multipronged approach encompassing the use of proxy-blocking services, international economic pressure, and the passage of an abbreviated version of the Global Online Internet Act.

Savvy Chinese Internet users already use proxy-blocking services such as Anonymizer. Although the funding for these programs may run against current United States public policy, this nation has had a long history of promoting anonymous speech and must continue to promote this in China. Moreover, against a background of radical political change and vaguely written law, interested Chinese citizens already use word of mouth to spread information and can easily spread information about Anonymizer and other similar services that can circumvent government censors.

The international community may leverage China's recent entry into the WTO against China to encourage a retreat from Internet censorship. While free market forces direct corporations into China and the lure of profits compel them to comply with Chinese laws, the international community must not forget that China's desire to join the world economy is reciprocal to the world's desire to invest in China. International economic pressure has the potential to effect substantial change in China.

Although this solution may lessen the extent of the human rights violations, it fails to regulate American corporations in China, especially those that cooperate with Chinese censorship laws. Here, the Global Online Freedom Act can play its role. If passed in an abbreviated form, the bill can apply fines against American companies that participate in Chinese censorship without involving the Department of State in the enforcement of American laws abroad.

---

208. "[T]he United States, China, and Europe are using their coercive powers to establish different visions of what the Internet might be. . . . The result is the beginning of a technological version of the cold war, with each side pushing its own vision of the Internet's future." GOLDSMITH & WU, *supra* note 98, at 184.

209. *See generally id.*; LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (arguing that the very architecture of cyberspace can be changed to address Internet-related economic and legal problems); Jonathan Zittrain, *Saving the Internet*, HARV. BUS. REV., June 2007, at 49, 55 (focusing on how domestic trends towards user-friendly Internet devices may stifle creativity).

V. CONCLUSION

Chinese censorship and the subsequent prosecution of its online writers presents a serious problem that continues to escalate each day as the Chinese firewall grows in complexity and sophistication. Although the Internet was once considered uncontrollable by any one nation, with the aid of American corporations China is succeeding in creating a second-tier Internet—one that increasingly delivers only news approved by the government. The complicity of these American corporations, coupled with the complacency of their shareholders, requires the United States and the international community to create and implement a solution to reintroduce freedom of speech in China.[210]

However, the chosen solution must consider the worldwide implications resulting from its implementation. Even though the Global Online Freedom Act in its current form would go against American public policy, the use of both proxy-blocking services and international economic pressure to create change in China would not. Instead, these recommendations would provide an effective short-term solution to circumventing Chinese Internet censorship.

210. One of Google's founders, Sergey Brin, recently admitted, "On a business level, that decision to enter China was a net negative based on our reputation in the rest of the world suffering." However, Google has not committed to a change in policy. Andrew Edgecliffe-Johnson, *Google Links Setbacks in China to Problems with Local Net Rivals*, FIN. TIMES, Jan. 27, 2007, at 8.