Washington International Law Journal

Volume 8 | Number 2

3-1-1999

Are You My Mommy, or My Big Brother? Comparing Internet Censorship in Singapore and the United States

Lewis S. Malakoff

ARE YOU MY MOMMY, OR MY BIG BROTHER? COMPARING INTERNET CENSORSHIP IN SINGAPORE AND THE UNITED STATES

Lewis S. Malakoff

Abstract: Governments across the globe are grappling to find an appropriate and effective way to regulate Internet activity. Singapore's experience with Internet regulation is particularly instructive, illustrating the inherent tension when a government simultaneously champions the Net's commercial, educational, and social potential while attempting to protect its population from material that offends the community's normative sensibility. Singapore has enacted regulations that require Internet Service Providers to filter content at the network level through the use of proxy servers. In addition, Singapore has issued an Internet Code of Practice that establishes the framework for acceptable speech in cyberspace. In the United States, Congress faces a similar struggle: constructing an appropriate legislative response to issues posed by the Internet while balancing competing interests of free speech and community values. Despite political, cultural, and social differences between Singapore and the United States, both nations' fledgling attempts to regulate the Internet have been driven by similar goals and have led to remarkably similar conclusions. Regulation in cyberspace presents challenges that transcend national idiosyncrasies and will potentially push divergent nations toward a common legal regime in which a limited market-driven response might provide the most effective instrument of control.

I. INTRODUCTION

The explosive growth of the Internet has spawned a new frontier of human communication. The ease with which information is distributed through cyberspace create exciting possibilities and unique challenges. The immediacy of communication, the relatively low cost of participation, and a potentially vast audience make the Internet a truly democratic medium in which anyone with a modicum of computer literacy can find a forum for expression. Internet communication draws together people from across the globe into a multi-national, multi-ethnic virtual commons where traditional jurisdictional boundaries might become obsolete.[1] According to John Perry Barlow of the Electronic Frontier Foundation, the Internet offers the "promise of a new social space, global and anti-sovereign, within which anybody anywhere can express to the rest of humanity whatever he or she believes without fear."[2]

---

[1] David R. Johnson & David Post, *Law and Boarders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1368-76 (1996).

[2] Jim Erickson, *www.Politics.com*, ASIAWEEK, Oct. 2, 1998, at 42, *available in* LEXIS, Asiapc Library, Asiaweek File.

On the other hand, the promise of electronic communication also delivers consequences because individuals now have unprecedented access to all types of information. As a result, governments around the world are grappling to find an appropriate and effective way to regulate Internet activity. Governments that traditionally suppress information and throttle dissent have found the Internet particularly threatening.[3] These countries, which have customarily attempted to restrict and control their citizens' access to all forms of media, have attempted aggressively to regulate the Internet.[4] Fear of the "dark side" of cyberspace is especially pronounced in some Asian nations, where many view the "Americanized" Internet culture as anathema to traditional Asian mores.[5] In these nations, censorship efforts have been aimed at preventing the erosion of "Asian values" perceived to be under siege by the infiltration of pernicious American elements.[6] According to the research head of a Malaysian securities firm, balancing the problems and opportunities of the Internet is particularly vexing for Southeast Asian countries that "want to reap the benefits of globalization and the information age [sic] while at the same time [keep] out 'moral hazards' like pornographic material, seditious speech and so on."[7]

Singapore's experience with Internet regulation is particularly instructive because it illustrates the inherent tension when a government simultaneously champions the Net's commercial, educational, and social potential while attempting to protect its population from material that offends the community's normative sensibility. The Singapore government has embraced many aspects of the Internet Age. Every Government ministry has its own World Wide Web site, computers link Singapore's entire civil service, and Singaporeans can even pay taxes online.[8] According to the Singapore Broadcast Authority's ("SBA")[9] official Web site, the

---

[3] *Id.* Countries such as China, Mynamar, and Vietnam all restrict Internet access to varying degrees. *Id.*

[4] *Censorship on the "Net": The View from Overseas,* NETWORK WORLD, Oct. 27, 1997, at 51, *available in* LEXIS, Busfin Library, Abi File.

[5] A. Shukor Rahman, *Another Bid to Regulate the Net,* NEW STRAITS TIMES (MALAYSIA), Feb. 16, 1998, at 20, *available in* LEXIS, Asiapc Library, Nstrtt File.

[6] Siti Rahil & Shuichi Nakamura, *Internet Braves Singapore's Tight Censorship Rule,* JAPAN ECON. NEWSWIRE, Aug. 24, 1996, *available in* LEXIS, Asiapc Library, JEN File.

[7] Teo Pho Keng & Oon Yeoh, *Neighbors Race to Become Asian IT Hub: Singapore, Malaysia, Plan Huge Internet Networks to Attract Investment,* NIKKEI WEEKLY, Nov. 17, 1997, at 21, *available in* LEXIS, Asiapc Library, Nikkei File.

[8] Erickson, *supra* note 2.

[9] Singapore Broadcast Authority, *How We Began* (visited Mar. 31, 1999) <http://www.sba.gov.sg/work/sba/about.nsf/pages/aboutsba> [hereinafter *How We Began*]. Following the privatization of Singapore's broadcasting industry, the SBA was established under the Singapore Broadcasting Authority Act, STATUTES OF THE REP. OF SING., Ch. 297 (1995) (Sing.), to regulate and promote broadcasting in Singapore. *Id.*

Agency's policies are designed to "encourag[e] a healthy and responsive environment for [the] Internet to thrive," while "develop[ing] and harness[ing] the full potential of the Internet."[10] Singapore business has also become increasingly "wired," as more than sixty percent of businesses composed of at least ten employees use electronic mail.[11] Computing and online communication are already woven into the fabric of Singaporean society. The Lion City boasts one of the highest computer literacy rates in the world,[12] along with one of the highest densities of Internet subscribers.[13] Additionally, Singapore has enthusiastically embraced the commercial potential of the Internet, aspiring to establish itself as the "Silicon Valley of Asia."[14]

Nevertheless, the Singapore government is both cognizant and wary of the many potentially destructive influences floating through cyberspace.[15] Eager to preserve normative "social values" and shield its population from the Net's most unseemly elements, the Singapore Broadcast Authority instituted an ambitious regulatory program in 1996, designed to control distribution and consumption of the Internet.[16] Since the regulations originally took effect, SBA officials have insisted that the government intends to regulate with a "light touch," without stifling Internet growth.[17] The SBA maintains a dual approach to Internet policy. It actively promotes Internet development, while at the same time limiting public access to content it considers offensive to Singapore's "community values."[18] In

---

[10] Singapore Broadcast Authority, *SBA and the Internet* (1999) (visited Mar. 31, 1999) <http://www.sba.gov.sg/work/sba/internet.nsf/pages/internetmain> [hereinafter *SBA and the Internet*].

[11] Teo Pho Keng & Oon Yeoh, *supra* note 7.

[12] *Id.*

[13] Siti Rahil & Shuichi Nakamura, *supra* note 6. In addition, the SBA reports that with about 600,000 subscribers as of February 1999, Singapore has one of the highest Internet penetration rates in the world. Singapore Broadcast Authority, *SBA's Approach to the Internet* (1999) (visited Mar. 31, 1999) <http://www.sba.gov.sg/work/sba/internet.nsf/ourapproach/1> [hereinafter *SBA's Approach*].

[14] Teo Pho Keng & Oon Yeoh, *supra*, note 7. Since 1996, the number of Web sites in Singapore has grown from 900 to over 5500. The SBA has placed a priority on increasing this number. *SBA's Approach*, *supra* note 13.

[15] *SBA's Approach*, *supra* note 13. On its Web site, the SBA notes that the Internet has "opened up a Pandora's box in terms of content which [sic] is unsuitable for children." *Id.*

[16] *SBA and the Internet*, *supra* note 10. On its Web site, the SBA states that its goal is "to develop and harness the full potential of the Internet while at the same time, maintain social values, racial, and religious harmony in Singapore." *Id.*

[17] Siti Rahil & Shuichi Nakamura, *supra* note 6. When the SBA introduced its regulatory program, George Yeo, Singapore's Minister for Information and the Arts, explained that the government would "regulate the Internet with a light hand. . . our objective is to promote it, not to impede its development." *Id. See also SBA and the Internet*, *supra* note 10.

[18] SINGAPORE BROADCAST AUTHORITY, INDUSTRY GUIDELINES ON THE SINGAPORE BROADCASTING AUTHORITY'S INTERNET POLICY para. 3 (Oct. 22, 1997), *available in SBA's Approach*, (visited Mar. 31, 1999) <http://www.sba.gov.sg/work/sba/internet.nsf/ourapproach/1> [hereinafter INDUSTRY GUIDELINES].

addition, the SBA recognizes the technical and legal complexity involved in regulating cyberspace; through its policies, the agency attempts to work in partnership with the community by emphasizing non-regulatory approaches such as public education, industry self-regulation, and the promotion of what it describes as "positive sites."[19]

In the United States, Congress faces a similar struggle: constructing an appropriate legislative response to issues posed by the Internet. As in Singapore, U.S. policy makers have labored to encourage technological growth while attempting to balance the competing interests of free speech and community values. Twice, Congress has passed legislation designed to regulate cyberspace and control Internet content.[20] However, these legislative efforts have yet to withstand judicial scrutiny as the courts have struck down portions of these laws under the First Amendment.[21] Although constitutional constraints have sharply limited Congress' ability to control activity on the Internet, legislators continue to seek a legitimate legislative formula.

This Comment will explain how, despite political, cultural, and social differences between Singapore and the United States, both nations' fledgling attempts to regulate the Internet have been driven by similar goals and have led to remarkably similar conclusions. Section II examines Singapore's Internet Regulation scheme, while Section III examines the failed efforts of the U.S. Congress to police Internet activity. Considering that a rule of law is only effective to the extent that it is enforced, Section IV explores liability under Internet regulation in both Singapore and the United States. Section V investigates the challenges encountered by the SBA in enforcing Internet rules and how this has limited Singapore's regulatory efforts. Section VI presents alternative models for how a state might regulate Internet content. Finally, Section VII concludes that the challenges of cyberspace transcend national idiosyncrasies and push divergent countries toward a common legal regime in which a limited market-driven response might provide the most effective instrument of control.

---

[19] *Id.* para. 3.b.

[20] *See* Communications Decency Act of 1996, Pub. L. 104-104, 110 Stat. 56 (1996) (codified in scattered sections of 47 U.S.C.); *see also* Child Online Protection Act, Pub. L. No. 105-277, Div. C, Title XIV, § 1403, 112 Stat. 2681-736 (1998) (codified at 47 U.S.C.A. § 231 (West Supp. 1999)).

[21] *See* Reno v. A.C.L.U., 521 U.S. 844 (1997) (holding that by prohibiting transmission of "obscene or indecent" material to minors under age 18 the Communications Decency Act impermissibly abridged First Amendment freedoms); *see also* A.C.L.U. v. Reno, 31 F.Supp.2d 473 (E.D. Pa. 1999) (enjoining United States Department of Justice from enforcing the Child Online Protection Act). *See* discussion *infra* notes 95-108 and accompanying text.

II. INTERNET REGULATION UNDER SINGAPORE LAW

A. *Singapore's Regulatory Framework: The Singapore Broadcast Authority Class Licence Notification*

Singapore has developed a reputation for efficient control over media and the flow of information.[22] Singapore's Constitution provides every citizen "the right to freedom of speech and expression."[23] However, the Constitution qualifies this right by permitting the government to pass laws that abridge free speech rights in specified instances where "necessary or expedient."[24] Consequently, Singapore's Parliament has passed laws that regulate broadcasting,[25] publication,[26] religious speech,[27] and sedition.[28]

Pursuant to the authority granted to it under the Singapore Broadcast Authority Act, the SBA has issued two principal regulations relating to the Internet: the Singapore Broadcasting Authority (Class Licence) Notification 1996 ("Class Licence Notification")[29] and the Internet Code of Practice ("Code").[30] These laws establish the framework for Singapore's effort to govern Internet activity and content beyond its existing speech laws. Under the regulations promulgated by the SBA, an Internet Service Provider ("ISP") is a company that provides its customers with a "main gateway" to the Internet.[31] An Internet Content Provider ("ICP"), on the other hand, can

---

[22] Ray Heath, *Lion Closes Net on Rogue Sites*, S. CHINA MORNING POST, Sept. 20, 1996, at 35, *available in* LEXIS, Asiapc Library, Schina File.

[23] CONST. OF THE REP. OF SING. art. 14 para. (1)(a).

[24] *Id.* art. 14 para. (2)(a). Article 14 para. (2)(a) provides that the Singapore Parliament may impose restrictions on the free speech rights conferred by the Constitution where "necessary or expedient in the interest of the security of Singapore or any part thereof, friendly relations with other countries, [and] public order or morality." *Id.*

[25] Singapore Broadcasting Authority Act, STATUTES OF THE REP. OF SING., ch. 297 (1995) (Sing.).

[26] Undesirable Publications Act, STATUTES OF THE REP. OF SING., ch. 338 (1985) (Sing.).

[27] Maintenance of Religious Harmony Act, STATUTES OF THE REP. OF SING., ch. 167A (1991) (Sing.).

[28] Sedition Act, STATUTES OF THE REP. OF SING., ch. 290 (1985) (Sing.).

[29] The Singapore Broadcasting Authority (Class Licence) Notification 1996, *available in SBA's Approach* (visited Mar. 31, 1999) <http://www.sba.gov.sg/work/sba/internet.nsf/ourapproach/1> [hereinafter Class Licence Notification]. This regulation, in operation as of July 15, 1996, was issued by the SBA under the power vested by Section 21 of the Singapore Broadcasting Authority Act, STATUTES OF THE REP. OF SING., ch. 297 (1995) (Sing.). *Id.* para. 1.

[30] The Internet Code of Practice, *available in SBA's Approach* (visited Mar. 31, 1999) <http://www.sba.gov.sg/work/sba/internet.nsf/ourapproach/1> [hereinafter Code]. This regulation, issued by the SBA under the power vested in it by Section 18 of the Singapore Broadcasting Authority Act, STATUTES OF THE REP. OF SING., ch. 297 (1995) (Sing.), took effect November 1, 1997. *Id.* para. 1. For discussion of the Code see generally *infra* notes 69-91 and accompanying text.

[31] Class Licence Notification para. 2. This includes:

a. an Internet Access Service Provider licensed under Section 26 of the Telecommunication Authority of Singapore Act (Cap. 323);

be any individual, corporation, or group that "provides any programme, for business, political or religious purposes on the World Wide Web through the Internet."[32] The Class Licence Notification requires all Service Providers and specified Content Providers to register with the SBA[33] and pay a license fee.[34] It also mandates that all ISPs and ICPs comply with the Internet Code of Practice.[35]

1. *Regulation of Internet Service Providers*

The first step in the SBA's effort to control Internet content involves filtering at the ISP level. To achieve this, the SBA has imposed technical standards requiring all ISPs to have in place the technical ability to comply with its regulations.[36] Traditional filtering approaches require systems (specialized software and hardware) that examine each page as it is downloaded by the end user.[37] Because large-scale application of this method would be unfeasibly slow, the SBA has encouraged ISPs to install and use proxy server technology.[38] Proxy servers, originally designed to speed access along Intranets, operate by storing a vast array of Web pages in memory.[39] This database, or cache, of Web sites includes those pages most frequently requested by users.[40] Under this system, a user surfing the Net does not connect directly with a distant Web site, but rather, receives a copy of the requested page, which the proxy server stores locally.[41] An ISP can

---

b. a localised Internet Service Reseller; or

c. a Non-localised Internet Service reseller.

Id. Also, according to the SBA, an Internet Service Reseller is one who provides public access to the Internet through ISPs and includes such organizations as schools, public libraries, and cybercafes. INDUSTRY GUIDELINES, *supra* note 18, para. 7. Singapore is currently served by three local ISPs which provide primary access to the Internet: SingNet, Pacific Internet and CyberWay. *Id.*

[32] *Id.* para. 2.

[33] *Id.* para. 4.2(1) (requiring all ISPs to register with the SBA within 14 days of providing service); para. 3(b) (requiring specified content providers to register within 14 days after the commencement of its service.). For a discussion of which ICPs are required to register with the SBA, see *infra* notes 64-68 and accompanying text.

[34] Class Licence Notification para. 4.2(1)(c).

[35] *Id.* para. 4.11-.12.

[36] Tong Ming Chien, *Device to Block Out Blacklisted Web Sites,* STRAITS TIMES (SING.), July 20, 1996, at 6, *available in* LEXIS, Asiapc Library, Strait File.

[37] *Id.* Traditional filtering at the service provider level requires the ISP to install additional computers, called "routers," which check each request made by a user. Such an approach is both expensive and inefficient, slowing down access for all users. *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] Lavinia Ng, *Cyber Trade Taking Root in Singapore: Arguments Remain on How Internet Regulation Affects Online Commerce,* NIKKEI WEEKLY, July 13, 1998, at 18, *available in* LEXIS, Asiapc Library, Nikkei File.

program a proxy server to update the pages in its cache automatically, storing only those pages considered legitimate.[42] In addition to enhancing access speed, the proxy server acts as an electronic traffic cop, allowing the ISP to control those pages that are stored, while blocking access to predetermined "objectionable" Web sites.[43]

Nevertheless, the SBA recognizes that such servers provide only a last resort and cannot effectively filter out all subversive content.[44] Singapore authorities also recognize that exclusive reliance on proxy server filtering is not feasible and might slow access speed and be a drag on Internet growth in Singapore.[45] Therefore, the agency has directed all ISPs to offer "Family Access Networks" that use filtering software at the network level to block access to objectionable content.[46] This optional service allows parents who are unfamiliar with the Internet or lack technical savvy to subscribe to a "cleaner, more sanitized Internet service."[47] In addition, Singapore's National Internet Advisory Committee ("NIAC")[48] recommended that additional filtering should be set up in places where children have access to the Internet, such as schools, community centers, and libraries.[49] The

---

[42] Tong Ming Chien, *supra* note 36.

[43] Lavinia Ng, *supra note* 41. According to Lee Lit Seang, SBA assistant director, "Although there are other ways of blocking out objectionable sites, using proxy servers helps ISPs control and censor Internet traffic better." Tong Ming Chien, *supra* note 36.

[44] *Naughty Sites Still Accessible: Device to Block Out Blacklisted Web Sites*, STRAITS TIMES (SING.), July 20, 1996, *available in* LEXIS, Asiapc Library, Strait File. Lee Lit Seang, SBA assistant director concedes that "parents are the first line of defence. . . the SBA censorship can only be the last resort." *Id.*

[45] *Singapore To Introduce Child-Safe Internet Service*, AGENCE FRANCE PRESSE, Mar. 17, 1998, *available in* LEXIS, News Library, Afpfr File.

[46] *Id.*. All three of Singapore's ISPs launched "Family Access" filtering services in 1998. *SBA's Approach, supra* note 13.

[47] *Id.* According to the SBA, "The optional service will filter out pornographic sites and provide an optional, hassle-free network-level solution to parents who are concerned with pornography on the Internet but are unfamiliar with the use of stand-alone filtering software such as CyberPatrol and NetNanny. This network-level filtering makes it more difficult for smart children to bypass or tamper with the filter settings." Singapore Broadcast Authority, *Tips for Parents* (visited Mar. 31, 1999) <http://www.sba.gov.sg/work/sba/internet.nsf/pages/tipsparents> [hereinafter *Tips for Parents*].

[48] NATIONAL INTERNET ADVISORY COMMITTEE, REPORT OF THE NATIONAL INTERNET ADVISORY COMMITTEE 1996/1997, *available in SBA and the Internet* (visited Mar. 31, 1999) <http://www.sba.gov.sg/internet.htm> [hereinafter NIAC REPORT1996/97]. Appointed by the Ministry of Information and the Arts in August 1996, the NIAC, comprised of 19 members, advises the SBA on "the regulation of electronic information services and the development of the industry . . . [and] assists SBA in the development of its regulatory framework for the Internet." *Id.* at para. 1.

[49] NATIONAL INTERNET ADVISORY COMMITTEE, REPORT OF THE NATIONAL INTERNET ADVISORY COMMITTEE 1997/1998, at Annex B *available in SBA and the Internet* (visited Mar. 31, 1999) <http://www.sba.gov.sg/internet.htm>. In the United States, similar efforts to regulate Internet access in public space have failed to withstand Constitutional scrutiny. Mainstream Loudoun v. Bd. of Trustees of Loudoun County Library, 24 F.Supp.2d. 552, 567 (E.D. Va. 1998) (holding that a Virginia community's attempt to equip Internet terminals in its public library with filtering software violated the First Amendment by restricting "what adults may read to a level appropriate for children").

agency has also embarked on an educational campaign, suggesting that subscribers provide parental supervision and/or employ filtering software such as Net Nanny on their home PCs.[50]

The SBA also requires that ISPs register with the agency, pay a license fee, comply with all Singapore laws, and abide by the applicable provisions of the Internet Code of Practice.[51] When this law was first enacted, some confusion existed regarding an ISP's duty to police and enforce the law, and ISPs requested further clarification from the SBA.[52] Singapore's NIAC agreed that there was ambiguity.[53] In its first annual report, the NIAC requested that the SBA more clearly articulate both the standard for "offensive" content[54] and an ISP's duty under the law.[55] Addressing these concerns, the SBA revised the Code of Practice in 1997.[56]

The new regulations make clear that ISPs are not required to search the Web proactively for objectionable content. Rather, they are only required to follow the directives of the SBA and deny access to any sites the agency identifies as "objectionable."[57] In general, as long as the Service Provider follows the directives of the SBA, it has met its duty of care under the Code.[58] An ISP discharges its duty when it denies access to content on the World Wide Web identified by the SBA as containing prohibited material.[59] With respect to newsgroups, an ISP discharges its duty when it refrains from subscribing to any newsgroup likely to contain prohibited material or "unsubscribes" from any newsgroup as directed by the SBA.[60] Furthermore, the SBA made clear that the Code does not require ISPs to search actively for objectionable Web sites[61] or monitor their subscribers' personal use.[62] Therefore, Singapore law treats an ISP more in the fashion

---

[50] Tong Ming Chien, *supra* note 36. The SBA recognizes that proxy servers only form a front line of defense and actively encourages parental supervision. *Id.*

[51] Class Licence Notification para. 4.2. For discussion of the Code and an ISP's duty under the Code, see generally *infra* notes 69-91 and accompanying text.

[52] *Advisory Board in Singapore Calls for Clearer Internet Rules*, DEUTSCHE PRESSE-AGENTUR, Sept. 25, 1997, *available in* LEXIS, News Library, DPA File.

[53] NIAC REPORT1996/97, *supra* note 48, para. 6.

[54] *Id.* at paras. 8-9.

[55] *Id.* at paras. 11-12.

[56] *Singapore Government to Revise Internet Regulatory Code*, DEUTSCHE PRESSE-AGENTUR, Oct. 20, 1997, *available in* LEXIS, News Library, DPA File.

[57] Edmund Tee, *Revised Internet Code Makes Taboo Areas Clear*, STRAITS TIMES (SING.), Oct. 23, 1997, at 3, *available in* LEXIS, Asiapc Library, Strait File.

[58] Code para. 3.

[59] *Id.* at para. 3(1).

[60] *Id.* at para. 3(2)(a-b).

[61] INDUSTRY GUIDELINES, *supra* note 18, para. 16; *see also* Tee, *supra* note 57.

[62] INDUSTRY GUIDELINES, *supra* note 18, para. 16. According to the SBA, its "purview covers the provision of material to the public. It is not concerned with what individuals receive, whether in the

of a library and less like a publisher or broadcaster, eliminating strict liability for third-party material and for objectionable content carried unknowingly over the ISP's equipment.[63]

2. *Regulation of Content Providers*

In addition to regulating Internet services in Singapore, the SBA also established regulations for Internet Content Providers.[64] The Class Licence Notification requires registration only by those content providers who are parties, bodies of persons, individuals engaged in the discussion of political or religious issues,[65] or those who provide an online newspaper for a subscription fee or other consideration.[66] According to the SBA, this policy does not intend to restrict religious and political speech, but rather aims to force content providers to be responsible and accountable for the views they promote online.[67] The SBA claims that registration of sites with political or religious content is necessary to prevent strife, given the multi-ethnic composition of Singapore society.[68]

Although the Class Licence Notification requires only a minority of ICPs to register with the SBA, all ICPs in Singapore must abide by the Internet Code of Practice.[69] The law further requires that all content providers make "best efforts" to ensure that all contributions to its site, such

---

privacy of their own home or at their workplace." *SBA's Approach, supra* note 13. The SBA further states that private communication, either via electronic mail or Internet Rely Chat (IRC), falls outside the scope of the regulations. *Id.*

[63] Code para. 3(5).

[64] Class Licence Notification para. 2. According to the SBA, an ICP is defined as:

> any individual in Singapore who provides any programme, for business, political or religious purposes on the World Wide Web through the Internet; or
>
> any corporation, group of individuals (including any association, business, club company, society, organisation or partnership, whether registrable or incorporated under the laws of Singapore or not) who provides any programme on the World Wide Web through the Internet, and includes any web publisher and web server administrator.

Id.

[65] *Id.* para. 4.3-4.

[66] *Id.* para. 4.4.a.

[67] INDUSTRY GUIDELINES, *supra* note 18, para. 9.

[68] Singapore Broadcast Authority, *Myths and Facts about SBA and the Internet, available at SBA's Approach, supra* note 13. Having experienced a series of race riots in the 1950s and 1960s Singapore is especially wary of the potential that the Internet could become a platform for "inflammatory and possibly insidious discussions which could incite religious and racial discord." Singapore Broadcast Authority, *Frequently Asked Questions, available in SBA's Approach supra* note 13. For further discussion of Singapore's regulation of Internet content and ICPs, see generally Sarah B. Hogan, *To Net or Not to Net: Singapore's Regulation of the Internet*, 51 FED. COMM. L.J. 429, 436-40 (1999).

[69] *SBA's Approach, supra* note 13.

as chats, postings, and so forth also conform with the applicable regulations.[70] Similar to an ISP, an ICP discharges its duty under the Code by denying access to prohibited material where directed to do so by the SBA,[71] choosing themes for private chat groups that are not prohibited,[72] denying contributions from others that contain prohibited materials,[73] and ensuring that its own programming does not include prohibited material.[74]

B. *Internet Code of Practice*

In November 1997, the SBA issued a revised Internet Code of Practice that outlines the obligations of ISPs and ICPs, and identifies the kind of content the Singapore community regards as offensive.[75] The central purpose of the 1997 revisions was to provide greater clarity, while fine-tuning the SBA's Internet regulation scheme.[76] Whereas the original Act was criticized for being overly broad and difficult to interpret, the revised Code was an attempt to clarify expectations of ISPs and ICPs.[77] The revised Code alleviated concerns about broad liability exposure, by explicitly outlining the extent and limit of the duty of care.[78]

In addition, the Code attempts to define more clearly what constitutes objectionable content by providing guidelines for determining whether specific content is prohibited.[79] Because it is impossible to create by statute an all-inclusive list of what might be considered objectionable, the Code provides what the SBA describes as "broad markers" of the type of content "offensive to the Singapore community."[80] Such material includes pornography, depictions of violence, and materials that may undermine Singapore's racial and religious harmony.[81]

The 1997 revision maintains the original broad intent, prohibiting material "objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited

---

[70] Class Licence Notification paras. 4.11-12.
[71] Code para. 3(4).
[72] *Id.* para. 3(3)(a).
[73] *Id.* para. 3(3)(b).
[74] *Id.* para. 3(3)(c).
[75] *Id.* para. 4.
[76] *Singapore Government to Revise Internet Regulatory Code, supra* note 56.
[77] Tee, *supra* note 57.
[78] Jason Tan, *New Net Rules Show S'Pore is Ready to Become Info Hub*, STRAITS TIMES (SING.), Oct. 25, 1997, at 65, *available in* LEXIS, Asiapc Library, Strait File.
[79] INDUSTRY GUIDELINES, *supra* note 18, at paras. 14-15.
[80] *Id.* para. 15.
[81] *Id.* para. 14.

by applicable Singapore laws."[82] However, the revised Code defines such content more specifically, outlawing a vast array of sexual content, including material depicting nudity or genitalia,[83] coercive or violent sex,[84] explicit sex,[85] and child pornography.[86] The Code also targets sexual behavior that deviates from the community's normative standard. It finds objectionable material that "advocates homosexuality or lesbianism, or depicts or promotes incest, pedophilia, bestiality, and necrophilia."[87] In the non-sexual arena, the Code targets material depicting extreme violence or cruelty,[88] and material that incites or endorses ethnic, racial or religious hatred, strife, or intolerance.[89] The Code does, however, take into consideration the material's potential medical, scientific, artistic, or educational value.[90] Through the revised Code, the SBA sharpened its definition of "objectionable," focusing on three principal targets: pornography, violence, and racial or religious intolerance.[91]

III. INTERNET REGULATION UNDER UNITED STATES LAW

In the United States, the rise of the Internet has been greeted with a mix of enthusiasm and concern similar to that in Singapore. However, in contrast to the experience in Singapore, U.S. courts have stymied Congress' attempts to regulate Internet content directly, holding these legislative efforts unconstitutional on First Amendment grounds.

A. *Censoring the Net, Round I: The Communications Decency Act and Reno I*

Attempts to regulate the Internet in the United States expose the inherent tension between the First Amendment's protection of free speech and Congress' intent to protect children from materials it considers harmful. The Communications Decency Act of 1996 ("CDA"), passed by Congress as

---

[82] Code para. 4(1).
[83] *Id.* para. 4(2)(a).
[84] *Id.* para. 4(2)(b).
[85] *Id.* para. 4(2)(c).
[86] *Id.* para. 4(2)(d).
[87] *Id.* para. 4(2)(e).
[88] *Id.* para. 4(2)(f).
[89] *Id.* para. 4(2)(g).
[90] *Id.* para. 4(3).
[91] Tee, *supra* note 57.

Title V of the Telecommunications Act of 1996,[92] was Congress' initial attempt to address this problem. Sweeping in scope, section 223 of the CDA prohibited and made criminal the knowing transmission of "obscene or indecent" material to anyone under the age of eighteen.[93] A second provision outlawed knowingly sending or displaying in a manner available to a person under eighteen "patently offensive" material.[94]

The Supreme Court struck down these two provisions in *Reno v. A.C.L.U.*, holding that the CDA was unacceptably broad and that the law placed an impermissibly heavy burden on protected speech.[95] Noting that the First Amendment protects expression that is "indecent but not obscene,"[96] the Court held that the CDA interfered with constitutionally protected speech.[97] The Court reasoned that the CDA was a "content-based regulation of speech," too vague to withstand constitutional scrutiny.[98]

B. *Censoring the Net, Round II: The Child Online Protection Act and Reno II*

Congress attempted to cure the CDA's constitutional defects with a subsequent piece of legislation, the Child Online Protection Act

---

[92] Communications Decency Act of 1996, Pub. L. 104-104, 110 Stat. 56 (1996) (codified in scattered sections of 47 U.S.C.).

[93] 47 U.S.C. § 223(a)(Supp. II 1996) (held unconstitutional in part by the United States Supreme Court in Reno v. A.C.L.U. 521 U.S. 844, 883 (1997)). Section 223(a)(B)(ii) prohibits an individual from transmitting "any comment, request, suggestion, proposal, image, or other communication which is obscene *or indecent*, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication." 47 U.S.C. § 223(a)(B)(ii)(emphasis added).

[94] 47 U.S.C. § 223(d) (held unconstitutional by the United States Supreme Court in *Reno*, 521 U.S. at 883). This provision prohibits use of an interactive computer service to either send or display, "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms *patently offensive as measured by community standards*, sexual or excretory activities or organs, regardless or whether the user of such service placed the call or initiated the communication." 47 U.S.C. § 223(d)(1)(A)-(B)(emphasis added).

[95] *Reno*, 521 U.S. at 879 (holding that the governmental interest to protect children from harmful materials does not justify an unnecessarily broad suppression of adult speech and that the CDA effectively suppresses a large amount of protected speech where less restrictive alternatives are available. The Court further notes that "the level of discourse reaching a mail box simply cannot be limited to that which would be suitable for a sandbox," (quoting Bolger v. Youngs Drug Products Corp., 463 U.S. 60, 74-75 (1983)).

[96] *Reno*, 521 U.S. at 874 (quoting Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989)).

[97] *Reno*, 521 U.S. at 874-79. However, finding the ban on "obscene" transmissions in 47 U.S.C. § 223(a)(1)(B)(ii) constitutional, the court utilized the Act's severing clause, 47 U.S.C. § 608 (1994), striking the words "or indecent" § 223(a)(B)(ii), while leaving the rest of § 223(a) intact. *Id.* at 883.

[98] *Reno*, 521 U.S. at 870-74.

("COPA").[99] In an attempt to fashion a law more narrowly tailored to a compelling state interest than the CDA, COPA takes aim solely at commercial operators of World Wide Web sites.[100] The law prohibits Web site operators from allowing minors access to "harmful" material, and it subjects violators to stiff criminal sanctions.[101] In addition, COPA requires the operator of a Web site to restrict minors' access to such material, by requiring the use of credit cards, adult personal identification numbers, digital age verification, or "any other reasonable measures that are feasible under available technology."[102] COPA also imposes a uniquely broad and novel standard for determining what is "harmful to minors," defining such material as that which is "obscene or that the average person, applying *contemporary community standards,* would find, taking the material as a whole and with respect to minors, is designed to appeal to, or . . . pander to, the prurient interest."[103]

Opponents of COPA struck first in the battle over the law's constitutionality. After an immediate challenge by the American Civil Liberties Union ("A.C.L.U.") and a consortium of Web site operators, a Pennsylvania district court enjoined the Department of Justice from enforcing COPA until a trial on the merits of the case.[104] Granting the request for injunctive relief, the court held that the plaintiffs were likely to succeed on the merits, finding a substantial likelihood that they would establish that the requirements of COPA would burden constitutionally protected speech.[105] Furthermore, the court held that the government was unlikely to prove that COPA was either narrowly tailored or the least restrictive means available to achieving its goal.[106] While recognizing a

---

[99] Child Online Protection Act, 47 U.S.C.A. § 231 (West Supp. 1999) (enforcement by United States Department of Justice enjoined in A.C.L.U. v. Reno, 31 Fd.Supp.2d. 473, 498 (E.D. Pa. 1999)).

[100] 47 U.S.C.A. § 231(a)(1). Under the statute, "a person shall be considered to make a communication for commercial purposes only if such person is engaged in the business of making such communications." 47 U.S.C.A. § 231(e)(2)(A). COPA further defines "engaged in the business" to mean a person "who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, . . . as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities . . ." 47 U.S.C.A. § 231(e)(2)(B).

[101] 47 U.S.C.A. § 231(a)(1)-(3). Under COPA violators face up to six months imprisonment and fines of up to $50,000. In addition, the statute also allows for additional civil penalties and even more substantial fines where the violation is intentional. *Id.*

[102] 47 U.S.C.A. § 231(c).

[103] 47 U.S.C.A. § 231(e)(6) (emphasis added).

[104] A.C.L.U. v. Reno, 31 F. Supp.2d 473 (E.D. Pa. 1999).

[105] *Id.* at 495 (holding that the "uncontroverted evidence showed" there is no way to restrict the access of minors without pre-screening all users).

[106] *Id.* at 497 (finding evidence that filtering software might, in practice, be more effective than COPA for protecting minors without imposing burdening constitutionally protected speech).

legitimate government interest in protecting minors, the court nevertheless noted that "the public interest is not served by the enforcement of an unconstitutional law."[107] The court aptly framed the complexity and tension underlying this case, and Congress' repeated attempts to regulate the Internet, concluding: "Perhaps we do the minors of this country harm if First Amendment protections, which they with age will inherit fully, are chipped away in the name of their protection."[108]

Consequently, U.S. law continues to treat Internet content in a manner similar to content provided by traditional media.[109] Until Congress can fashion legislation that regulates Internet speech without offending First Amendment rights, it cannot place a special patrol on the information superhighway.[110]

IV. ENFORCING CENSORSHIP: LIABILITY IN CYBERSPACE

Both Singapore and the United States have attempted to control the Internet through direct regulation.[111] However, in both nations, the extension and enforcement of private rights also shapes online conduct.[112] The Internet is a virtual world in which nearly any liability for private conduct might arise. However, because the Internet is principally a medium of mass communication, defamation provides the most likely cause of action in cyberspace.[113]

---

[107] *Id.* at 498.

[108] *Id.*

[109] Reno v. A.C.L.U. 521 U.S. 844, 870 (1997) (reasoning that "our cases provide no basis for qualifying the level of First Amendment scrutiny that should apply to this medium.").

[110] *A.C.L.U. v. Reno*, 31 F. Supp.2d at 498. For further discussion of the status of the law in the United States involving liability of ISPs for third party content, see *infra* notes 130-157 and accompanying text.

[111] See *supra* notes 22-91 and accompanying text for discussion of the law in Singapore and *supra* notes 92-110 for discussion of the law in the United States.

[112] Tang Liang Hong v. Lew Kuan Yew & Anor 1998-1 Sing. L. Rep. 97, 1997 SLR LEXIS 215 (Sing. C.A.) (applying Singapore's common law of defamation to statements published first in the Straits Times and later republished on the newspaper's World Wide Web site). *Hong* illustrates how private liability arising under the law of defamation constrains speech. *Id.* at para. 117. The Singapore Court of Appeal noted that freedom of speech is neither absolute nor totally unrestricted. *Id.* Rather, "freedom of expression is perfectly legitimate so long as it does not encroach upon the realm of defamation." *Id.* For discussion of how common law rules have shaped ISP liability in the United States see *infra* notes 134-157 and accompanying text.

[113] David R. Sheridan, *Zeran v. AOL and the Effect of Section 230 of the Communications Decency Act Upon Liability for Defamation on the Internet*, 61 ALB. L. REV. 147, 149 (1997). The revolutionary nature of Internet communication offers unprecedented opportunity for reckless individuals to harm others "by propagating false and defamatory statements around the world at the speed of light." *Id.* at 151. For discussion of how defamation claims have helped provide the basis for establishing liability for ISPs in the United States see *infra* notes 130-157 and accompanying text.

A state may proscribe or protect particular speech through its allocation of common law liability among private parties.[114] Where the law vests rights in individuals, an aggrieved party may act as a private regulator and enforce state-sanctioned standards of conduct.[115] In this fashion, tort liability functions as a tool of the state by creating strong incentives for individuals to act in accordance with normative standards.[116]

However, the unique nature of the Internet makes it difficult to determine fault and assign liability. Internet communication strains established doctrine of vicarious liability, as the ISP defies traditional categorization as either publisher or distributor.[117] Assigning liability for Internet speech is further complicated because a speaker may lurk anonymously in the vast expanse of cyberspace and an ISP cannot feasibly track and monitor the volume of material it carries each day.[118]

Both Singapore and the United States have responded to these challenges by reducing liability exposure for ISPs.[119] However, regulation of individual speakers and Internet Content Providers may not require different legal treatment from traditional media.[120] In Singapore, the Internet Code of Practice, along with existing speech laws, provide a comprehensive legal basis for controlling Internet speech that takes place within Singapore's borders.[121] In the United States, despite the failure of both the CDA and COPA, a court is free to assess traditional common law liability when the

---

[114] New York Times v. Sullivan, 376 U.S. 254, 265 (1964) (holding that enforcement of state libel law by Alabama state courts constitutes state action, even in a civil lawsuit between private parties). Writing for the majority, Justice Brennan noted, "It matters not that the law has been applied in a civil action and that it is common law only. . . The test is not the form in which state power has been applied but, whatever the form, whether such power has in fact been exercised." *Id.* at 265. *See also* Ruzicka v. Conde Nast Publications, Inc., 733 F.Supp 1289, 1295-96 (D. Minn. 1990) (holding that state law placement of the burden of proof in a civil contract claim involving the publication of sensitive information constitutes state action in which speech is deterred through fear of liability).

[115] Keith N. Hylton, *Implications of Mill's Theory of Liberty for the Regulation of Hate Speech and Hate Crimes*, 3 U. CHI. L. SCH. ROUNDTABLE 35, 38 (1996). Hylton notes that speech may be regulated either by "public officials [who] enforce command and control statutes that specify the range of lawful conduct," or by "liability rules that create incentives for private individuals to enforce constraints on . . . conduct." *Id.*

[116] Lingens v. Austria, 8 Eur. Ct. H.R. (ser. a) at 407, para. 46 (1986). In *Lingens*, the European Court of Human Rights held that Austrian law requiring proof of the truth of a defamatory opinion violated the convention's free speech provisions. *Id.* at para. 55. The court noted the chilling effect of civil liability, finding that Austria's law created a burden of proof regarding value judgements that is "impossible of fulfilment and it infringes the freedom itself." *Id.* at para. 46.

[117] Andrew J. Slitt, *The Anonymous Publisher: Defamation of the Internet After Reno v. American Civil Liberties Union and Zeran v. America Online*, 31 CONN. L. REV. 389, 390, 412-413 (1998).

[118] *Id.* at 414.

[119] *See infra* notes 158-166 and accompanying text.

[120] Robert M. O'Neil, *The Drudge Case: A Look at Issues in Cyberspace Defamation*, 73 WASH L. REV. 623, 634 (1998).

[121] *See supra* notes 22-28, 75-91 and accompanying text.

speech is not protected under the First Amendment and a speaker with editorial control can be identified.[122]

A. *Liability of Internet Service Providers Under Singapore Law*

The revised Code clarified ISPs' and ICPs' duties under Singapore law and relieved them of liability for content beyond their control.[123] Underlying the SBA Code's relaxation of private liability is a practical compromise recognizing that technological and physical limitations minimize the agency's ability to enforce its regulations effectively.[124]

Nevertheless, Singapore's law does not relieve an Internet author of liability under the Code or Singapore's speech laws.[125] Furthermore, Singapore's common law of defamation exerts additional control over speech that extends to Internet publication.[126]

The SBA extends purveyors of third-party content sufficient freedom to operate by reducing liability exposure for material beyond their control.[127] They are required to block access to online content only when directed to do so by the SBA, or when they discover prohibited material in the normal course of exercising editorial duties.[128] Because liability does not attach when ISPs or ICPs have used "best efforts" to monitor their services,[129] the revised Code provides them with reassurance and incentive to self-regulate.

B. *Liability of Internet Service Providers in the United States*

Through legislation and judicial decision, the United States has adopted a similar approach in assessing the responsibility and liability of an Internet Service Provider. Section 230 of the Communications Decency

---

[122] O'Neil, *supra* note 120, at 634-35.

[123] Code para. 3(3)-(5).

[124] *See also infra* notes 167-176 and accompanying text.

[125] See *supra* notes 75-91 and accompanying text for discussion of the Internet Code of Practice; *supra* notes 22-28 and accompanying text for discussion of speech laws under Singapore's Constitution and Statutes.

[126] Lee Kuan Yew v. Jeyaretnam JB (No. 1) 1990 Sing. L. Rep. 688, 1990 SLR LEXIS 345, *53 (Sing. High Ct.) (holding that "freedom of speech is in terms of art. 14 [of the Constitution of the Republic of Singapore] subject to or restricted by the law of defamation"). Rejecting the rule of New York Times v. Sullivan, 376 U.S. 254 (1964), Singapore's High Court noted that the framers of Singapore's Constitution, "had after all deliberate considerations chosen the policy of balancing freedom of speech and expression against certain other individual rights, including not least the protection of reputation." *Id.* at *53-*57. *See also*, Goh Chok Tong v. Tang Liang Hong, 1997-2 Sing. L. Rep. 641, 1997 SLR LEXIS 43, *58 (Sing. High Ct.).

[127] Code para. 2-3. *See also supra* notes 57-63 and accompanying text.

[128] Code para. 3. *See also supra* notes 57-63 and accompanying text.

[129] Code para. 2-3.

Act[130] and subsequent case law interpreting this provision, grants ISPs broad immunity from harm caused by third-party content or comments carried over their equipment.[131] In addition, this statute shields an ISP from liability for any action taken to filter potentially harmful content.[132]

Section 230 adopted as federal law the emerging majority view that an ISP is neither directly nor vicariously liable for the content or comments carried over its equipment.[133] In *Religious Technology Center v. Netcom*, the defendant online service provided Internet connectivity to the operator of a Bulletin Board Service ("BBS") critical of the Church of Scientology.[134] After the BBS operator posted portions of writings by the late founder of the church, L. Ron Hubbard, the Religious Technology Center, as holder of the copyright to Hubbard's work, brought an action against Netcom for copyright infringement.[135] The court denied the plaintiffs' motion for a preliminary injunction, holding that an ISP was not liable for direct infringement where users made and stored unauthorized copies on its equipment.[136] The court found that Netcom, an ISP which "does not create or control the content of information available to its subscribers" took no affirmative steps that directly resulted in the infringing activity.[137] The

---

[130] 47 U.S.C. § 230(c)(2) (Supp. II 1996). The statue provides that:

1) Treatment of publisher or speaker. No 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.

2) Civil liability. No provider or user of an interactive computer service shall be held liable on account of —

A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, whether or not such material is constitutionally protected; or

B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Id. Although the Supreme Court struck down the "indecency" and "patently offensive" provisions of the Communications Decency Act in Reno v. A.C.L.U. 521 U.S. 844, 883 (1997), the Act included a severability clause, 47 U.S.C. § 608 (1994), that allowed § 230 to remain intact and in force after *Reno*. *See generally* Elizabeth deGrazia Blumenfeld, *Publisher Liability in Cyberspace*, *in* CABLE TELEVISION LAW 1998: TWO YEARS AFTER THE 1996 TELECOMMUNICATIONS ACT 1998, at 763, 765 (PLI Pat., Copyrights, Trademarks, & Literary Prop. Course Handbook Series No. 509, 1998).

[131] 47 U.S.C. § 230(c)(1). *See also* Zeran v. American Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (unanimously upholding the federal district court's finding that "distributor" liability was merely a subspecies of "publisher" liability and that § 230 of the CDA expressly immunized the defendant service provider, AOL); Blumenthal v. Drudge, 992 F.Supp. 44, 52 (D.C. Dist. 1998).

[132] 47 U.S.C. § 230(c)(2).

[133] *See generally* Blumenfeld, *supra* note 130.

[134] Religious Technology Center v. Netcom, 907 F.Supp. 1361 (N.D. Cal. 1995).

[135] *Id.* at 1365-66.

[136] *Id.* at 1373.

[137] *Id.* at 1368.

Netcom court established that liability for content does not attach to an ISP where the provider acts only as a conduit for information, offering its customers unfiltered, unmonitored Internet access and connectivity.

In a similar case, *Cubby, Inc. v. Compuserve, Inc.*, the court relieved the defendant ISP of liability, holding that where an ISP is merely a distributor of information, it may be held liable only when it knew or had reason to know of defamatory statements carried over its service.[138] In this case, the plaintiff sued defendant Compuserve for allegedly defamatory statements made by a publication carried in Compuserve's electronic library.[139] The court found that Compuserve had no editorial control over the publication and acted as a distributor, similar to "a public library, bookstore, or newsstand."[140] Finding that the plaintiff failed to show that Compuserve knew or had reason to know of the statements, the court granted Compuserve's motion for summary judgment.[141]

However, where an ISP has held itself out as "edited" or "clean," some courts were willing to impose a stricter standard of care prior to the CDA.[142] In *Stratton Oakmont, Inc. v. Prodigy Services Company*, the New York Supreme Court held that an ISP can be liable when it actively monitored and edited content.[143] In this case, the court found the defendant ISP, Prodigy, liable for defamation arising from comments made about the plaintiff on a moderated bulletin board hosted by Prodigy. The court distinguished this case from *Compuserve*, finding that Prodigy held itself out as "an on-line service that exercised editorial control over the content of messages posted on its bulletin board service."[144] The court held that Prodigy exposed itself to greater liability than those ISPs acting only as "distributors" by making a "conscious choice" to gain the commercial and competitive benefits of editorial control.[145]

Under section 230 of the Communications Decency Act, Congress codified the basic approach of *Netcom* and *Compuserve* and rejected the policy of *Prodigy*, by granting ISPs immunity from tort liability, even where the provider attempted to exercise editorial discretion or restrict access to

---

[138] Cubby, Inc. v. Compuserve, Inc., 776 F.Supp. 135, 141 (S.D.N.Y. 1991).

[139] *Id.* at 137.

[140] *Id.* at 140.

[141] *Id.* at 144.

[142] Stratton Oakmont, Inc. v. Prodigy Services Company, 1995 N.Y. Misc. Lexis 229, *13 (N.Y. 1995) (holding that where Internet service provider held itself out as a service exercising editorial control, provider was exposed to tort liability).

[143] *Id.* at *12.

[144] *Id.* at *3, *10.

[145] *Id.* at *13.

"objectionable" material.[146] In addition to providing a broad exemption from "publisher liability" for third-party content carried over an ISP's network,[147] the law explicitly superceded *Prodigy*, removing the specter of publisher liability when an ISP opts to self-regulate and screen out potentially offensive material.[148] Congress intended 47 U.S.C. § 230(c)(3) to relieve ISPs from liability for third-party content[149] while removing all disincentives for ISPs to self-police.[150]

Judicial interpretation of this provision has further defined an ISP's duty under the law, establishing broad immunity from civil claims.[151] In *Blumenthal v. Drudge*, a Federal District Court granted defendant America Online's ("AOL") motion for summary judgment in a defamation action even though the Service Provider had purchased and actively promoted the allegedly defaming work of cyber gossip columnist Matt Drudge.[152] Sidney Blumenthal, a former journalist and aide to President Clinton, filed suit against both Drudge and AOL, after the online service carried a column in which Drudge published unsubstantiated accusations of spousal abuse by Blumenthal.[153] The court found that in hiring and promoting Drudge, AOL had engaged in activities beyond that of a mere distributor.[154] Nevertheless, the court held that section 230 of the CDA protected AOL from liability, despite the fact that it stood to gain financially from its contractual relationship with Drudge.[155]

As a result of these cases, an ISP faces substantially less liability exposure than traditional print media.[156] Relieved of responsibility for third-party content, an ISP is now free to amass and distribute vast amounts of

---

[146] 47 U.S.C. § 230(c)(2) (Supp. II 1996).

[147] 47 U.S.C. § 230(c)(1).

[148] 47 U.S.C. § 230(c)(2). The statute expressly states that "It is the policy of the United States . . . to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. § 230(b)(4). *See also* H.R. CON. REP. NO. 104-458, at 194 (1996) ("[O]ne of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material.").

[149] 47 U.S.C. § 230(c)(1).

[150] 47 U.S.C. § 230(b)(4). *See also supra* note 148 and accompanying text.

[151] Zeran v. American Online, Inc., 129 F.3d 327 (4th Cir. 1997); *see generally* Blumenfeld, *supra* note 130.

[152] Blumenthal v. Drudge, 992 F. Supp. 44, 51-52 (D.C. Dist. 1998).

[153] *Id.* at 46.

[154] *Id.* at 51 (noting that in the absence of § 230, the plaintiff, Blumenthal, would likely have had a valid claim against AOL given AOL's affirmative promotion of Drudge and its contractual right to exercise limited editorial control).

[155] *Id.* at 51-52 (holding that an ISP's immunity under § 230 constitutes a policy choice by Congress that preempts "publisher liability" under the common law).

[156] Sheridan, *supra* note 113, at 155, 179.

information without danger of incurring direct liability. By holding that section 230 of the CDA exempts the ISP from liability as either a publisher or distributor, *Blumenthal* and *Zeran* provide ISPs the option of creating an unchecked, free speech zone. On the other hand, by explicitly superceding *Prodigy*, section 230 allows ISPs the freedom to moderate content and offer "sanitized" service without exposure to a heightened standard of care.[157]

C. *The Convergence of U.S. and Singapore Law: Limited Liability for Internet Service Providers*

The U.S. Congress and courts appear to have reached the same conclusion as the Singapore government, characterizing ISPs as disseminators of information, while relieving them from the threat of civil liability. Both the United States and Singapore have created a legal structure designed to enlist the help of private ISPs in monitoring Internet activity and filtering "objectionable" content.[158] Singapore offers ISPs incentives to help the agency meet its objective of creating a sanitized online environment by granting ISPs relief from its exacting standards.[159] Similarly, section 230 of the CDA and the emerging U.S. case law allow an ISP in the United States the freedom to self-regulate with impunity.[160] The law enables an ISP to build networks rich with proprietary content produced by third-parties and provides incentives to create and market filtered online alternatives.[161]

This policy choice recognizes the reality that given the volume of information traveling over any given computer network, an ISP cannot efficiently transmit data while adequately monitoring content.[162] The SBA relieved Singapore's service providers from liability for third-party content because it was both impractical and unreasonable to hold the providers to such a high standard of care.[163] Furthermore, the U.S. cases demonstrate that imposing liability on Service Providers for the content on their networks creates strong disincentives for exercising even minimal editorial control.[164]

Internet Service Providers offer a unique mix of services. While an ISP displays some characteristics of traditional broadcast media, it also

---

[157] *See supra* notes 148-150 and accompanying text.
[158] *See supra* notes 127-129, 156-157 and accompanying text.
[159] *See supra* notes 127-129 and accompanying text.
[160] *See supra* notes 130-131 and accompanying text.
[161] *See supra* notes 156-157 and accompanying text.
[162] David J. Loundy, *Computer Information Systems Law and System Operator Liability*, 21 SEATTLE U.L. REV. 1075, 1091 (1998).
[163] *See infra* notes 167-176 and accompanying text.
[164] *See supra* notes 142-145 and accompanying text.

functions in a manner more akin to a utility. An ISP has the potential to offer both proprietary content and provide a window to the unlimited array of resources housed in cyberspace. Although an ISP might occasionally play a role in promoting or developing third-party content (as in *Blumenthal*), often service providers assume a far more passive position, acting more like a "common carrier" moving "data from one computer to another with no regard for the information being transferred."[165] Consequently, Congress has provided ISPs statutory immunity with respect to third-party content, superceding duties arising under state tort law.[166]

V. SINGAPORE INTERNET REGULATION IN PRACTICE: ENFORCEMENT IN "SLEEP MODE"

A. *Practical and Technical Limitations on Filtering*

Although Singapore passed ambitious regulatory programs for censoring cyberspace, actual enforcement of the law has lagged. One commentator described Singapore's enforcement as lapsing into "sleep mode."[167] The SBA's passive enforcement of its Code demonstrates the unique problems presented by the Internet as a medium and the limitations of filtering technology. Although server-level filtering via proxy server technology allows a modicum of control over the flow of information, this approach is insufficient given the Internet's unprecedented scope and constantly evolving nature.[168]

Despite the SBA's broad authority to censor Internet activity, the agency has adopted an approach it describes as a "light touch."[169] The Internet Code of Practice empowers the SBA to identify and block access to "objectionable" sites. However, the SBA has asserted this authority sparingly, limiting its "blacklist" to only one hundred "high-impact" pornography sites.[170] Recognizing the sprawling, fluid nature of cyberspace,

---

[165] Loundy, *supra* note 162, at 1091.

[166] *See supra* notes 154-157 and accompanying text.

[167] Rahman, *supra* note 5.

[168] *See supra* note 44 and accompanying text.

[169] *SBA and the Internet*, *supra* note 10.

[170] Ng, *supra* note 41. According to the SBA, "The list, which contains such sites as www.Playboy.com, is updated several times per year." *Id.* However, the actual list is available only to authorized personnel at the ISPs, because the SBA has chosen to keep the information confidential under the Official Secrets Act of Singapore. Sintercom, *The Singapore R(A) Url Hunt: Background* (visited, March 31, 1999) <http://www.sintercom.org/hunt/background.html>. Sintercom, a group of Internet activists have posted a list of sites they have discovered to be blocked by the SBA. This list of twenty Web sites includes Web sites for U.S. adult magazines such as www.playboy.com and www.hustler.com,

the SBA urges individual users to practice self-regulation while as a "token gesture," it keeps the list of banned sites at an even one hundred.[171]

Although political and religious sites are required to register under the Class Licence Notification, the SBA claims it does not intend either to censor or ban them.[172] Rather, the SBA asserts that it wants merely to hold individuals and organizations accountable for the views they promote and espouse.[173]

Content filtering at the server level can only be as effective and comprehensive as the censors employed to evaluate and identify the myriad of sites on the Web. Although Singapore could address this problem by employing an army of censors to monitor constantly the Internet's vast terrain, it has opted instead to apply a more cooperative approach, stressing public education and industry self-regulation.[174] As part of the SBA's aggressive public education effort, the Agency has created a "Tips for Parents" page on its Web site, offering information on the strengths and dangers of the Internet, strategies for additional filtering and supervision, and a list of Web sites it considers appropriate for children.[175] In addition, the agency encourages parents to subscribe to "Family Service Networks" for additional network-level filtering.[176]

B. *Commercial Concerns Limit Vigilance of Enforcement Effort*

Relaxed enforcement of the SBA's regulations is partially related to broader concerns for Singapore's image in the international marketplace.[177] Although wary of the more pernicious side of the Net, Singapore's leadership has placed a high priority on Internet development and has made a concerted effort to become an important Asian hub for the information

---

commercial pornographic sites such as www.pleasure.com and www.persiankitty.com, and adult verification services such as www.adultcheck.com, www.adultpass.com, and www.validate.com. Sintercom, *The Singapore R(A) Url Hunt: Banlist* (visited, March 31, 1999) <http://www.sintercom.org/hunt/banlist.html>. Sintercom discovered that the SBA also blocked a legitimate site, public.calweb.com that is merely a typical IRC chatroom. *Id.*

[171] Ng, *supra* note 41.

[172] INDUSTRY GUIDELINES, *supra* note 18, para. 9. *See also supra* notes 67-68 and accompanying text.

[173] Industry Guidelines, supra note 18, para. 9. See also supra notes 67-68 and accompanying text.

[174] *SBA's Approach*, *supra* note 13.

[175] *Tips for Parents*, *supra* note 47. While recommending that parents take adequate measures to supervise their children's online time, the SBA remains a steadfast promoter of the Web's educational benefits. "The Internet is a vast resource pool for information with tremendous reach and impact. It is a veritable treasure chest of knowledge, all ready for the taking." *Id.*

[176] *See supra* notes 46-47 and accompanying text.

[177] Joshua Gordon, *East Asia, too, is Giving up on Internet Censorship*, INT'L HERALD TRIB., Nov. 30, 1998, at 8, *available in* LEXIS, News Library, IHT File.

technology industry.[178] Singapore officials recognize that financial leadership in the "Information Age" requires a free flow of data, and that strict regulation can stifle innovation and hinder business development.[179]

To attain regional leadership in the industry, Singapore has aggressively recruited infotech and e-commerce firms.[180] These efforts have been harmed by an international perception that Singapore was engaged in a program of widespread, draconian censorship.[181] This perception led Singapore's National Internet Advisory Committee to recommend that the SBA promulgate its rules with greater specificity[182] and better promote its positive goals for facilitating Internet development.[183] As a result, Singapore's initial regulatory zeal may have been tempered by pressure from the international business community.[184]

C. *The Symbolic Value of Regulation*

Despite its "light touch,"[185] the Singapore Internet Code of Practice retains some potency, both as a symbol and as an instrument of control. In practice, Singapore's Internet censorship regulations are merely "symbolic acts, rather than a practical attempt to enforce its policy."[186] The fact that the Code remains in force allows the government a legitimate means for controlling Internet activity if and when it chooses to do so.

To date, ISPs and ICPs have generally abided by the SBA's guidelines, and the SBA has not "taken action against anyone for objectionable content on the Internet."[187] Furthermore, the Agency has banned only a sliver of the Web

---

[178] Tan, *supra* note 78.

[179] Peter Montagnon, *Quest for a Way Through the Storm*, FIN. TIMES (LONDON), Mar. 31, 1998, *available in* LEXIS, Asiapc Library, Fintme File.

[180] Erickson, *supra* note 2.

[181] Steve Levy, *The Hot New High Tech Cities*, NEWSWEEK, Nov. 9, 1998, at 45.

[182] NIAC REPORT 1996/97, *supra* note 48, para. 8.

[183] *Id.* at para. 28. According to Associate Professor Bernard Tan, chairman of the Internet Advisory Committee, "Such ambiguity must be clarified so that Singapore's plan to become an internet hub is not hindered. . . . We will need more than just technical expertise and a good infrastructure. We need creative talents to come up with exciting content, design interesting web-pages, graphics, etc. . . ." Chua Chin Hon, *Rules Have Not Hindered Internet, but Fine Tune Them Says Advisory Body*, STRAITS TIMES (SING.), Sept. 26, 1997, at 2, *available in* LEXIS, Asiapc Library, Strait File. However, some industry observers suspect that competition from Malaysia in the race to achieve high-tech primacy may have motivated the SBA to relax enforcement of its Internet regulations. Teo Pho Keng & Oon Yeoh, *supra* note 7.

[184] Erickson *supra* note 2. According to Garry Rodan, senior research fellow at Murdoch University's Asia Research Center, "The very negative reaction from international business [to the original rules] [indicated] that this was not functional as a way to promote commercial aspects of their technology." *Id.*

[185] *See supra* note 17 and accompanying text.

[186] Ng, *supra* note 41.

[187] *SBA's Approach*, *supra* note 13. However, in 1986 a Singaporean was fined the equivalent of $44,000 for possession of pornography, some of which he had downloaded from the Internet. *The Cutting*

sites it could potentially designate as "objectionable" under the Internet Code of Practice.[188] Nevertheless, the existence of a valid regulatory scheme provides the government with a statutory basis to exert state power on occasions it deems necessary. The value of a regulation may be measured beyond the scope of its effectiveness, especially when regulating cyberspace. According to Professor Lawrence Lessig, "A regulation need not be absolutely effective to be sufficiently effective. It need not raise the cost of the prohibited activity to infinity in order to reduce the level of that activity quite substantially."[189]

Although Singapore's regulatory apparatus cannot entirely block access to objectionable content, where "regulation increases the cost to this kind of information, it will reduce access to this information."[190] Singapore has minimally enforced the Code; nevertheless, the Code carries symbolic weight, defining the outer limits of the community's tolerance while serving notice of the government's desire to enforce these limits.

VI. MODES OF ENFORCEMENT: MODELS OF INTERNET REGULATION

A regulatory scheme is at its core an exercise of state power, restricting individual liberty to further the state's policy objectives. However, the state may assert itself in a variety of ways, taking into account the legitimacy of the regulatory arrangement and the likelihood that the regulation will be effective.[191] Both Singapore and the United States have attempted to regulate Internet activity, and despite significant differences in culture and political systems, both nations' regulatory programs have been hampered by similar challenges. Although Singapore law permits certain forms of censorship,[192] the Internet's nonlinear, amorphous, and almost infinite scope makes comprehensive regulation nearly impossible. Despite the SBA's ambitious plan, its program of Internet regulation has had minimal practical effect.[193] In the United States, efforts to control cyberspace have been checked not only by technological limitations but also by constitutional constraints.[194] Yet, despite these challenges, government can play some role in helping shape its citizens'

Edge; Testing the Boundaries; Countries Face Cyber Control in their Own Ways, L.A. TIMES, Jun. 30, 1997, *available in* LEXIS Asiapc Library, LAT File.

[188] *See supra* notes 170-171 and accompanying text.

[189] Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1405 (1996).

[190] *Id.*

[191] See *supra* notes 167-190 and accompanying text for discussion of how technical limitations, commercial concerns, and symbolic value have shaped enforcement of Singapore's Internet laws.

[192] *See supra* notes 26-28 and accompanying text.

[193] *See supra* notes 169-173 and accompanying text.

[194] *See supra* notes 95-98, 104-108 and accompanying text.

online environment. This section will explore various models of state action and evaluate each paradigm as to its applicability for regulating Internet content.

A. *Father Knows Best: The State as a Benevolent Parent*

With this paradigm, the State supplies a normative moral code, a filter through which information must pass before reaching the end user. Essentially, this is Singapore's original plan; require all access through heavily regulated proxy servers capable of filtering out objectionable content.[195] An advantage of this approach is that network-level filtering eliminates the jurisdictional problem of trying to regulate ICPs situated beyond a state's borders.[196] Rather than attempting to control the infinite array of ICPs that exist in cyberspace, regulatory efforts can be focused on a limited number of ISPs, situated squarely within the state's jurisdiction.

In practice, however, the prophylactic value of such an approach is questionable, even in a community as small as Singapore. Assuming that proxy server technology advanced to the point where the servers could accommodate large national networks, comprehensive immunization from objectionable content would still require significant human resources, including a vast staff of censors, constantly monitoring the Web and updating the servers' cache. In addition, the proxy server's performance would exponentially decline as more sites were blocked, because the server must check each user request against the list of prohibited Web sites.[197] The fact that Singapore has chosen to ban only a symbolic list of one hundred pornographic sites[198] demonstrates the inherent difficulty in identifying, monitoring, and policing cyberspace. Although network-level filtering might prove useful in small, close-knit communities, this approach is unlikely to work effectively on a national level.

B. *Big Brother is Watching: The State as Enforcer of Moral Standards*

Although Singapore law permits the state to establish standards of morality,[199] enforcing such standards on the Internet has proven both

---

[195] *See supra* notes 36-43 and accompanying text.

[196] Johnson & Post, *supra* note 1, at 1374. A local authority asserting rights to regulate content accessed by its citizens is likely to be frustrated by companies operating in cyberspace from a physically remote location, beyond its jurisdictional reach. *Id.*

[197] *See generally* Hogan, *supra* note 68, at 445-46.

[198] *See supra* note 170 and accompanying text.

[199] *See supra* note 192 and accompanying text.

impracticable and futile. Practical and technical considerations have minimized the state's ability to enforce its initially ambitious regulatory program vigorously.[200] Meanwhile, strict regulation has proven burdensome for local business, slowing connectivity while harming Singapore's image in the international marketplace.[201] Therefore, Singapore has backed away from its initial policies, relaxing civil liability for ISPs[202] while opting not to enforce its Code against private users.[203]

Singapore's Internet Code of Practice remains legally operative, and the specter of enforcement carries some symbolic weight,[204] leading Singapore based ICPs to comply generally with the regulations.[205] Nevertheless, a nation cannot legitimately legislate beyond its jurisdiction.[206] Singapore-based ICPs constitute only a mere ripple in a vast ocean, and full compliance with the Code would have marginal aggregate impact. Recognizing "a limit to what domestic legislation can achieve in the face of a global and borderless medium like the Internet," the SBA "strongly emphasises public education and industry self-regulation in addition to government regulation."[207]

C. *I'm OK, You're OK: Peer-Review and Industry Self Regulation*

Similar to the television and motion-picture industries, a government could encourage self-regulation by entrusting industry members and organizations to establish and enforce Internet standards more aggressively. Under this approach, ICPs and ISPs could establish industry standards for online content and institute their own methods for enforcement. Such an approach is already underway in Singapore, where the SBA has attempted to achieve its goal of "creat[ing] an environment in which self-regulation might flourish."[208] Similarly, in the United States, ratings systems developed by private parties are proliferating.[209]

---

[200] *See supra* notes 167-168 and accompanying text.

[201] Gordon, *supra* note 177.

[202] *See supra* notes 57-63, 123-129 and accompanying text.

[203] *See supra* note 62 and accompanying text.

[204] *See supra* notes 185-190 and accompanying text.

[205] *SBA's Approach*, *supra* note 13. According to the SBA's Web site, "service and content providers have generally abided by the guidelines." *Id.*

[206] Johnson & Post, *supra* note 1.

[207] *SBA's Approach*, *supra* note 13.

[208] *SBA's Approach*, *supra* note 13. As part of its effort to encourage industry self-regulation, the SBA has actively embraced content classification under the Platform for Internet Content Selection ("PICS") system developed by the World Wide Web Consortium. The SBA "urge[s] content providers in Singapore to support this effort by labeling their sites as part of industry self-regulation." *Id.* The SBA has led the way, affixing a seal to its own web site that indicates it has been self-rated under the RASCi system. *SBA and the Internet*,

However, private ratings systems offer a far from perfect solution and even if a single system were to become standard, significant problems would remain. The breadth and democratic nature of the Internet ultimately limits the effectiveness of any ratings system, because blocking software works perfectly only when all sites are rated.[210] On the World Wide Web, virtually anyone possessing moderate computer literacy can set up a site and compete with mega-media conglomerates on a reasonably level playing field. As a result, it is unlikely that even the most comprehensive rating service could continuously monitor and rate the entire World Wide Web.[211] Furthermore, it is impossible to craft an objective, value-neutral system of censorship; all filtering and rating systems necessarily incorporate distinct value judgments, blocking speech based on the system's internal political and social biases.[212]

Exclusive reliance on voluntary self-rating is unrealistic, as few content providers are likely to have sufficient incentives for participation.[213] Although compulsory self-rating might prove moderately effective in a small, tightly controlled nation such as Singapore, a nation can only regulate within its own jurisdiction.[214] Therefore, the international character of the Internet is likely to undermine this approach because it would be impossible to mandate use of any particular standard.

Inevitably, any system designed to rate and filter Internet content will either be overinclusive or underinclusive. A system permitting access to unrated material is ineffective, whereas a system that unilaterally blocks unrated material will deny access to innocuous and potentially valuable speech.[215] As a result, content rating systems could end up stripping the Internet of the medium's most compelling characteristics, breadth and diversity, leading to a flat online environment composed only of commercially produced content.[216] Although rating systems offer a promising, less restrictive alternative to overt content regulation, where

---

supra note 10. However, PICS do not provide substantive standards for Internet content. Rather, "PICS consists of technical specifications that provide Internet standards for rating formats. . . PICS is analogous to specifying the place on a package that a label should appear and the size of the label, with specifying what the label should say." Ari Staiman, *Shielding Internet Users from Undesirable Content: The Advantages of a PICS Based Rating System*, 20 FORDHAM INT'L L.J. 866, 882-83 (1997).

[209] Johathan Weinberg, *Rating the Net*, 19 HASTINGS COMM. & ENT. L.J. 453, 454-55 (1997).

[210] *Id.* at 470.

[211] *Id.* at 471. Weinberg further points out that "the sites most likely to be ephemeral are also among the most likely to carry sexually explicit material." *Id.*

[212] *Id.* at 481.

[213] *Id.* at 472.

[214] Johnson & Post, *supra* note 1.

[215] *Id.* at 470.

[216] *Id.* at 476-77.

strictly implemented, these systems impose identifiable social costs, by sharply reducing access to valuable, idiosyncratic speech.[217]

D. *Toward a Market-Based Alternative: Empowering Communities and Individuals to Patrol the Net*

Although the Internet belies direct, heavy-handed regulation, government can nevertheless play an important role in helping communities and individuals create ideal online environments. Similar to traditional media, active parental supervision leads to the safest online environment. Although state action is unlikely to alter significantly the type of material available on the Internet, certain measures can empower parents to select and tailor Internet service to fit their values.

In Singapore, at the direction of the SBA, all three ISPs now offer "Family Access Networks" that filter out additional pornographic and "undesirable" sites at the server level.[218] These services offer consumers a simple, network-level alternative to unrestricted access.[219]

In the United States, impunity from civil liability has freed ISPs either to filter or not, depending on market preferences.[220] By relieving ISPs from the haunting specter of civil liability, Congress is allowing the ISPs to create and provide the type of services the market most desires.[221]

Given the variety of barriers to effective Internet filtering, a market-driven approach might prove to be the most promising long-term solution in both nations. Although this model requires substantial parental supervision, it allows each family to control the type of content it receives. In a market that allows private entities to self-regulate, a family may either subscribe to an online community with shared values or use filtering software to shape a personalized Internet environment tightly aligned with its own value preferences. Although Internet censorship by government authorities might be impractical or even pernicious, a marketplace populated by informed and equipped consumers could wield substantial clout. Market pressures could regulate Internet content by forcing consumers and ISPs to create clearly delineated zones of cyberspace where "content or conduct acceptable in one 'area' of the Net may be banned in another."[222]

---

[217] *Id.* at 483.
[218] *Singapore to Introduce Child-Safe Internet Service, supra* note 46.
[219] *See supra* notes 46-47 and accompanying text.
[220] *See supra* notes 156-157, 160-161 and accompanying text.
[221] *See supra* notes 156-157 and accompanying text.
[222] Johnson & Post, *supra* note 1.

VII. CONCLUSION

The unique challenge presented by the Internet has led governments across the globe to embark on ambitious regulatory schemes. The experience with Internet regulation in both Singapore and the United States teaches valuable lessons about this new medium and the best way to harness its power within the law. Although both nations passed comprehensive legislative packages, the principal concern was limiting access to pornography. For different reasons, the regulations have failed in both nations.

In Singapore, the SBA discovered that the Internet's vast, decentralized nature rendered comprehensive censorship virtually impossible to achieve. As a result, the SBA has retreated from its initial program and focused on more modest goals such as encouraging industry self-regulation and empowering families.[223] In the United States, congressional efforts to regulate the Internet have been stymied by First Amendment concerns.[224]

Although constrained by different forces, the net result in both countries has been similar. Even where the law constitutes a legitimate exercise of state authority, broad regulations aiming to censor Internet content have proven impossible to enforce.[225] One approach to taming the Net is holding an ISP liable for the entire online environment it provides. However, in both Singapore and the United States this policy has been explicitly rejected, and ISPs in both countries face no direct liability for content carried and distributed over their services.[226]

The explosive growth of Internet communication poses unique challenges for government regulators. The examples in this Comment suggest that although a state might be tempted to unleash its heavy artillery and enter the fray with a comprehensive regulatory program, perhaps a more limited response would prove most effective. No single entity, either public or private, can possibly canvas, rate, and monitor the entire World Wide Web. As a result, the best instrument of control might be the pressure of an open marketplace in which consumers may select the ISP or filtering software that best accommodates their values and preferences.

---

[223] *See supra* notes 167-168, 174-176 and accompanying text.
[224] *See supra* notes 95-98, 104-108 and accompanying text.
[225] *See supra* notes 167-168 and accompanying text.
[226] *See supra* notes 157-166 and accompanying text.

A revolutionary technology, the Internet challenges our present conception of state intervention and regulation. However, as the state adjusts to previous advances in communications technology, existing institutions of governance will also adapt to this medium.[227] At this stage of the Internet's development, a government seeking to tame the wilds of cyberspace would be well served to recognize the powerful forces limiting effective government action. Nevertheless, as the examples of Singapore and the United States demonstrate, a state can contribute to the evolution of a healthy Internet environment. A practical approach consists of a partnership between the state, private purveyors, and end users, in which the state provides the education and tools necessary to empower individuals to control their own Internet access.

[227] David G. Post, *The Internet, the State, and the Consent of the Governed*, 5 IND. J. GLOBAL LEGAL STUD. 521, 522 (1998).