CODE RED: RESPONDING TO THE MORAL HAZARDS FACING U.S. INFORMATION TECHNOLOGY COMPANIES IN CHINA

Marc D. Nawyn*

---

* J.D. Candidate 2008, Columbia University School of Law; M.Phil. 2001, The Graduate Center of the City University of New York; B.A. 1997, Ramapo College. The author thanks Professors Benjamin Liebman and Katharina Pistor as well as Sylvie Goursaud, Michael Grunfeld, Allison Snyder and the staff of the Columbia Business Law Review for their many helpful comments and suggestions throughout the writing and editing process.

This paper surveys the nature and extent of China's control over the Internet, the problems it creates for U.S. Information Technology ("IT") companies doing business in the country, and various proposals on how to deal with them. It focuses on several controversial developments among major U.S. IT companies with ties to China, including Google's announcement that it would launch a censored version of its popular search engine for Chinese Internet users, Microsoft's decision to remove a controversial blog from the Chinese version of its MSN Spaces, and Yahoo!'s involvement in the identification and imprisonment of Chinese journalist Shi Tao, who used the company's email service to send politically sensitive documents abroad. It tentatively concludes that Chinese Internet users would be worse off, on the whole, if U.S. IT companies were prohibited from doing business in China and considers various forms a regulatory regime might take to prevent some of the more egregious examples of collaboration. After considering the prospects of both self-regulation and legislation, it comes out in favor of a hybrid approach involving the development of an industry-wide code of conduct propped up by legislation designed to deter noncompliance. Significant attention is devoted in the process to demonstrating the theoretical advantages of this hybrid approach within the conceptual space afforded by contemporary views of the natures of both the State and the corporation. Noting the limits to this approach as a model for the regulation of transnational business, it ends by suggesting the need for the development of something like a stakeholder theory of the modern State.

I. INTRODUCTION

U.S. Information Technology ("IT") companies have been selling computer hardware in China with mixed results since the late 1970s.[1] In 1998, Yahoo! launched a Chinese language version of its search engine and became the first major U.S. IT company to begin competing with China's domestic Internet Content Providers ("ICPs") for a stake in the country's emerging market for Internet-based products and services. Since then, Microsoft, Google, and others have followed suit.

It would be difficult to overstate just how attractive the prospects of doing business in China are for foreign ICPs. According to the China Internet Network Information Center ("CNNIC"), a non-profit organization formed under the direction of China's Ministry of Information Industry ("MII"), there were 123 million Internet users in China as of June 30, 2006.[2] This number was up from the 620,000 users CNNIC reported when it first began keeping track in October 1997.[3] Dr. Charles Zhang, chairman and CEO of Sohu.com, a Chinese web portal providing users with one stop access to news, entertainment, shopping, e-mail, wireless messaging, and web searches, puts the figure at somewhere between 150

[1] IBM sold its first mainframe to China in 1978. John H. Maier, *Information Technology in China*, 20 ASIAN SURVEY 860, 872 (1980). In an effort to promote the development of its own computer manufacturing industry, China imposed high tariffs on computer imports and frequently required foreign manufacturers operating within China to enter into joint ventures with its domestic companies. Failing to establish itself within the market, IBM entered into such a joint venture in 1984. Kenneth L. Kraemer & Jason Dedrick, *Enter the Dragon: China's Computer Industry*, COMPUTER, Vol. 35, No. 2, Feb. 2002, at 30-31.

[2] CHINA INTERNET NETWORK INFO. CTR. [hereinafter CNNIC], 18TH STATISTICAL SURVEY REPORT ON THE INTERNET DEVELOPMENT IN CHINA (July 2006), *available at* http://www.cnnic.net.cn/download/2006/18threport-en.pdf.

[3] CNNIC, STATISTICAL REPORT OF THE DEVELOPMENT OF CHINESE INTERNET (Oct. 1997), *available at* http://www.cnnic.net.cn/download/manual/en-reports/1.pdf.

to 200 million.[4] In either event, China boasts more Internet users today than any other country but the United States.[5] Given the population disparities between the two nations and the fact that the number of Internet users in China has increased by 18% for each of the past two years,[6] it is not a question of if, but when China will assume the top spot. With China's growth rate in per capita disposable income attaining double digits in 2006[7] and Zhang's claim that Chinese Internet users spend more time online than their American counterparts,[8] it is easy to see why U.S. IT companies might be eager to enter the market.

While the potential upside for U.S. IT companies able to get a foothold in China's Internet industry is admittedly huge, there are certain moral hazards unique to China's technology sector that have proven especially difficult for these companies to navigate. Because China's national firewall makes accessing foreign websites a slow and often hit-or-miss affair, ICPs hoping to cultivate a broad Chinese user base are effectively forced to set up shop within the country itself. Once there, however, they become entangled

[4] Natalie Pace, Editorial, *China Surpasses U.S. in Internet Use*, FORBES.COM, Apr. 3, 2006, http://www.forbes.com/2006/03/31/china-Internet-usage-cx_nwp_0403china.html. Zhang contends that because the CNNIC conducts its surveys over fixed phone lines, it underreports the number of younger users, who are more likely to rely solely on mobile phones. *See id.*

[5] There are presently 210 million Internet users in the U.S. *See* INTERNET WORLD STATS, USAGE AND POPULATION STATISTICS: TOP 20 COUNTRIES WITH THE HIGHEST NUMBER OF INTERNET USERS, http://www.Internetworldstats.com/top20.htm (last visited Feb. 23, 2007). By comparison, Japan, in third place, has an estimated 86 million users, while Germany, in fourth, has 51 million. *Id.*

[6] Pace, *supra* note 4.

[7] John Ng, *China's Economy Still Sizzling*, ASIA TIMES ONLINE, Jan. 26, 2007, http://www.atimes.com/atimes/China_Business/IA26Cb03.html.

[8] The figure has been suggested to be as high as 16:1. *See* Pace, *supra* note 4. As the U.S. figure is based on time spent per month on Yahoo! rather than the Internet as a whole, this is almost certainly wrong. *Id.* Nevertheless, three of the top ten most visited websites in the world are Chinese-Sohu.com, Baidu.com and Sina.com. *Id.*

in an elaborate regime of censorship and surveillance in which their full and active cooperation is expected.

In the following sections, this Note will consider in greater detail the nature and extent of China's control over its citizens' use of the Internet and the role U.S. IT companies have played in facilitating it. The Note will then address the issue of what, if anything, should be done to prevent these companies from playing that role in the future. While ultimately coming down on both theoretical and practical grounds in support of a hybrid self-regulatory/legislative approach that would require U.S. IT companies doing business in China to adopt a policy of complete disclosure when forced to censor content and to refrain from storing users' personal information on servers within the country, we acknowledge that the effectiveness of these solutions depends to a large extent on what China does in response. It may, for example, forbid companies from disclosing to users what it requires them to filter. It may also force them to retain customer records onsite and make them available on demand as a condition for doing business in the country. This Note argues that while the disclosure requirement is negotiable, U.S. IT companies should never be permitted to reveal the identities of political dissidents or anyone else not guilty of an internationally recognized violation of criminal law.

II. CHINESE INTERNET REGULATION

China's censorship of political and religious speech on the Internet takes two broad forms. First, it relies on the state's monopoly over the physical infrastructure of its large-scale domestic networks and their links to the outside world to filter what its citizens can view.[9] Second, it assures self-censorship on the part of Internet service and content providers, as well as end-users, through an extensive collection of laws and regulations that govern both access to

[9] Eric Harwit & Duncan Clark, *Shaping the Internet in China: Evolution of Political Control over Network Infrastructure and Content*, 41 ASIAN SURVEY 377, 378 (2001).

and content available on the Internet and are enforced by a frequently draconian array of civil and criminal penalties.[10] After a brief introduction to the mechanics of Internet filtering, this Note will take a closer look at how these two aspects of China's Internet policy are implemented.

A. Internet Filtering: An Introduction

"Internet filtering" is an umbrella term that covers a number of related methods for controlling the material users can access on the Internet.[11] The most prevalent form of filtering typically involves blocking users from accessing specific Internet Protocol ("IP") addresses.[12] This is accomplished through the use of either inclusion filters or exclusion filters.[13] Inclusion filters employ "white lists" to designate IP addresses users are permitted to visit.[14] Users are blocked from visiting any site not on the list.[15] Exclusion filters, on the other hand, use "black lists" to designate sites users may not visit.[16] Users are free to access any address not on the list.[17]

Inclusion and exclusion filters are particularly susceptible to the two basic flaws of Internet filtering in general: over-blocking and under-blocking.[18] By restricting access to sites at the IP address level, these filters prevent users from viewing any unobjectionable content that might also be housed on the site.[19] This tendency to over-block is especially true of inclusion filters, as white lists can hardly be expected

[10] *Id.*

[11] OPENNET INITIATIVE, INTRODUCTION TO INTERNET FILTERING, http://www.opennetinitiative.org/index.php (last visited Mar. 10, 2007) (follow "Internet Filtering" link under "Resources" menu) [hereinafter ONI, INTRODUCTION].

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

to keep pace with the rapid expansion of valuable and innocuous Internet real estate. Exclusion filters, by contrast, are particularly prone to under-blocking, as black lists can hardly be expected to keep pace with the equally rapid expansion of the Internet's less seemly neighborhoods.[20]

Recently, Internet filtering technology has started to rely more and more on "content analysis." Content analysis works by preventing users from accessing any site containing certain keywords, phrases, or even images.[21] This has two advantages over the blocking techniques discussed above. First, it does away with the need to maintain and constantly update lists of sites users may or may not visit, thus preventing significant under-blocking.[22] Second, it permits much more finely grained filtering than can be achieved by blocking sites at the IP address level.[23] Thanks to advances in computer power, content analysis filters can be designed to detect forbidden words, expressions, or other "content" within the IP packets traveling between the user's computer and the targeted site and prevent them from being received on either end.[24] This type of content-based "packet filtering" enables users to receive "uncontaminated" packets from sites that would otherwise be blacklisted altogether, thus reducing the over-blocking associated with traditional filtering techniques.[25] It has been compared to "censoring out individual sentences within books, as opposed to censoring entire books themselves."[26] Internet filters are used at various levels, from individual terminals, private

[20] Black lists can be updated through automated web searches; however, this once again raises the specter of over-blocking. *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] China uses Cisco Systems' 12000 series routers, which possess significant packet filtering technology. OPENNET INITIATIVE, INTERNET FILTERING IN CHINA IN 2004-2005 7, http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf (last visited Mar. 10, 2007) [hereinafter ONI, INTERNET FILTERING].

[25] ONI, INTRODUCTION, *supra* note 11.

[26] *Id.*

networks, and ISPs at the local and organizational levels to the physical infrastructure forming the backbone of the Internet at the national level, including the gateway routers that facilitate access to foreign networks.[27] For the most part, they are designed to prevent the spread of viruses and other malicious code[28] as well as of web-based criminal activities such as the production and distribution of child pornography.[29] They are also used by parents to restrict what their children are exposed to online[30] and by businesses seeking to encourage employee productivity by limiting access to non-work-related sites and activities.[31] A number of nations around the world use filters to curtail the free and open expression of political and religious speech.[32] As we will see, China has by far the most extensive and sophisticated of such filtering regimes, employing some or all of the filters discussed above at each of the levels just mentioned.[33]

B. Regulation at the National Level

Critics have dubbed the centerpiece of China's filtering strategy at the national level "The Great Firewall of

---

[27] *Id.*

[28] HUMAN RIGHTS WATCH, "RACE TO THE BOTTOM": CORPORATE COMPLICITY IN CHINESE INTERNET CENSORSHIP 9 (2006), http://www.hrw.org/reports/2006/china0806/china0806web.pdf.

[29] AMNESTY INT'L, UNDERMINING FREEDOM OF EXPRESSION IN CHINA: THE ROLE OF YAHOO!, MICROSOFT AND GOOGLE 4-5 (2006), http://web.amnesty.org/library/index/engPOL300262006.

[30] Australia's Internet Industry Association maintains a list of "family friendly filters" on its website at http://www.iia.net.au/index.php (last visited Jan. 12, 2007) (follow link for "IIA Guide for ISPs" under "Most Read" menu; list will appear on far right).

[31] Jonathan Zittrain & Benjamin Edelman, *Documentation of Internet Filtering Worldwide*, http://cyber.law.harvard.edu/filtering/ (last visited Jan. 12, 2007).

[32] *See* Global Online Freedom Act of 2006, H.R. 4780, 109th Cong. §105(a)(3)(B) (2006) (identifying Burma, China, Iran, North Korea, Tunisia, Uzbekistan, and Vietnam as "Internet-restricting countries.") [hereinafter Global Online Freedom Act].

[33] ONI, INTERNET FILTERING, *supra* note 24, at 3.

China."[34] The goal was to unite all the major Chinese networks[35] into a single intranet that could be insulated from the global Internet through a series of gateways that would control the flow of information between China and the outside world.[36] China planned to achieve this goal through precisely the kind of IP address blocking and content filtering methods described above.[37]

As ambitious as this filtering scheme sounds, it was not entirely farfetched. From the outset, major network development in China was the exclusive province of the government.[38] Initially, this was because it was limited to the academic sector, which was already regulated by various government agencies.[39] As the economic value of the Internet became apparent, these agencies used their expertise in and control over the infrastructure of existing academic networks (especially their bandwidth) to dominate the market for commercially viable ones.[40] In May of 1995, roughly eight years after the creation of its first academic computer networks, China began offering commercial Internet access to state and private corporations, as well as individuals, through the Ministry of Posts and Telecommunications' ("MPT") ChinaNET.[41]

The MPT acted largely as a wholesale provider of Internet bandwidth, leasing use of its data lines, as well as the ChinaNET name, to regional service providers, including

---

[34] The phrase was coined by Geremie R. Barme & Sang Ye, *The Great Firewall of China*, WIRED, June 1997, at 138. It is frequently confused with the so-called "Golden Shield," an elaborate surveillance project currently being developed. *See* GREG WALTON, CHINA'S GOLDEN SHIELD: CORPORATIONS AND THE DEVELOPMENT OF SURVEILLANCE TECHNOLOGY IN THE PEOPLE'S REPUBLIC OF CHINA 1 (2001), http://www.ddrd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF

[35] By 2001, China had nine major interconnecting networks. Harwit & Clark, *supra* note 9, at 385

[36] Walton, *supra* note 34, at 18.

[37] *Id.* at 18-20.

[38] *See* Harwit & Clark, *supra* note 9, at 382-387.

[39] *Id.* at 382-384.

[40] *Id.* at 390.

[41] *Id.* at 388.

state-owned telephone companies and, in short order, private ISPs.[42] Today, ISPs in China connect to the Internet through one of nine state-licensed Internet Access Providers ("IAPs"),[43] which, in turn, are regulated by MII. MII was formed out of a merger of MPT and several other agencies in 1998 to supervise China's Internet infrastructure and to run networks connected to the worldwide Internet.[44]

While its ownership and control of the physical infrastructure of the nation's Internet backbone does give China greater control over the content entering (and leaving) the country than would have been the case if these were in private hands, this power is not by itself sufficient to achieve the degree of control desired by China over the content its citizens can access. Users can simply circumvent the firewall by connecting to proxy servers outside China and using them to connect to a blocked site.[45] Because in such a case all transmission of suspect data occurs outside the firewall, there is nothing to trigger a block.[46] Of course, once the authorities discover a proxy server, access to it can be prevented. Since the locations of new proxy servers are disseminated on a daily basis through China's Internet underground, however, this will not be a problem for savvy users.[47]

Furthermore, firewalls do not prevent access to information already inside a network.[48] As we have already seen, however, much of China's domestic commercial

---

[42] *Id.*

[43] ONI, INTERNET FILTERING, *supra* note 24, at 6.

[44] *Id.* at 5-6.

[45] Alfred Hermida, *Behind China's Internet Red Firewall*, BBC News, Sept. 3, 2002, http://news.bbc.co.uk/1/hi/technology/2234154.stm

[46] For a brief tutorial on how proxy servers work, *see* ProxyServerPrivacy.com, Proxy Server, http://www.proxyserverprivacy.com/proxy-server.shtml (last visited Jan. 13, 2007).

[47] Tom Zeller Jr., *How to Outwit the World's Internet Censors*, N.Y. TIMES, Jan. 29, 2006, at 42. A 2005 survey conducted by the Chinese Academy of Social Sciences revealed that less than 3% of Chinese Internet users make frequent use of proxy servers. Over 70% reported never using them. *See* HUMAN RIGHTS WATCH, *supra* note 28, at 15.

[48] ProxyServerPrivacy.com, *supra* note 46.

networks are owned by regional ISPs, both public and private.[49] China therefore depends on their cooperation in filtering content that does not have to pass through the national firewall.[50]

C. Other Regulations

Since 1994, Chinese officials have promulgated over sixty different sets of regulations governing the use of and access to the Internet.[51] These regulations in turn have authorized at least twelve different governmental agencies[52] to oversee China's growing number of ISPs, ICPs, websites (including blogs), Internet cafes, and end users.[53] This oversight has typically taken the form of licensing and content monitoring requirements, backed up by severe fines and possible criminal penalties for violators.[54]

1. ISPs and ICPs

ISPs must be licensed by MII.[55] They are required to keep records of their users' personal information, including

---

[49] Harwit & Clark, *supra* note 9, at 388.

[50] HUMAN RIGHTS WATCH, *supra* note 28, at 11.

[51] HUMAN RIGHTS WATCH, FREEDOM OF EXPRESSION AND THE INTERNET IN CHINA: A HUMAN RIGHTS BACKGROUNDER 1 (2001), http://www.hrw.org/backgrounder/asia/china-bck-0701.pdf.

[52] ONI, INTERNET FILTERING, *supra* note 24, at 8.

[53] According to CNNIC's July 2006 Report, there were at the time 2,950,500 registered domain names and an estimated 788,000 websites operating in China. CNNIC, *supra* note 2, at 4-5. On top of that, there are approximately 113,000 Internet cafes. Zhang Di, *PC Maker Clicks with Net Cafes*, CHINA DAILY.COM.CN, Apr. 4, 2006, http://www.chinadaily.com.cn/bizchina/2006-04/04/content_559164.htm. The number of ISPs and ICPs is harder to calculate. As of early 2000, there were about 300 ISPs and 1000 ICPs. *Increase in Number of ISP Business License Issued*, PEOPLE'S DAILY ONLINE, Jan. 27, 2000, http://english.people.com.cn/english/200001/27/eng20000127T190.html. In its 2002 contribution to China's Tenth Five-Year Plan, MII projected a combined total of 5000 ISPs and ICPs by the end of 2005. *The Program of Information Industry during "tenth five-year plan,"* ASIAINFO DAILY CHINA NEWS, Sept. 7, 2001.

[54] *See* ONI, INTERNET FILTERING, *supra* note 24, at 9-18.

[55] *Id.* at 9.

names, account and phone numbers, and IP addresses, and they are responsible for any content they display.[56] For-profit ICPs must apply for special business licenses, while non-profit ICPs must file official records.[57] Any ICP seeking to provide a forum for electronic communication, such as a bulletin board system ("BBS"), must seek the permission of MII.[58] In addition, they must restrict access to registered users and retain records of all user activities for sixty days.[59] MII also requires ISPs to immediately remove and report any suspect posts.[60] Failure to abide by any of these requirements may result in fines, license revocations, and criminal sanctions for employees.[61]

2. Websites

In September of 2000, China's State Administration of Industry and Commerce began requiring all commercial websites to register with an electronic database maintained by its Beijing office.[62] This requirement was motivated not so much by a concern about content as by a desire to protect intellectual property rights in well-known website names and to avert any confusion that would likely result if those same names were subsequently registered by different owners at the domain level.[63] In March 2005, MII began

[56] *Id.* at 9-10.

[57] *Id.* at 10.

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] The American Chamber of Commerce People's Republic of China, *SAIC Takes Charge of Website Administration*, http://www.amcham-china.org.cn/amcham/show/content.php?Id=217&menuid=04&submid=04 (last visited Feb. 23, 2007).

[63] Xue Hong, *Domain Name Dispute Resolution in China*, 18 TEMPLE INT'L & COMP. L.J. 1, 23-24 (2004). This problem arose as domain names initially could only be registered in English, with the corresponding websites bearing Chinese characters. Once domain names could be registered using Chinese characters, opportunists could register the names of well-known Chinese websites as their domain names, thereby diverting traffic from those sites to their own.

requiring the registration of all non-commercial websites with independent domain names as well.[64] Any owner failing to register an affected website by June 30 of that year would be subject to fines ranging from between $600-$1200 U.S. dollars[65] and would have their sites shutdown.[66] Additionally, ISPs are required to monitor the websites they host and are subject to similar fines for failing to block access to unregistered sites.[67] The new policy is believed to be a response to the widespread proliferation of weblogs in China in recent years.[68] OpenNet speculates that one of its primary effects will be to encourage greater self-censorship among website and blog owners, who will now have one less layer of protection between them and the state.[69]

3. Internet Cafes

In China, as in many other developing nations, the cost of accessing the Internet from home or of even owning a computer at all can be prohibitively high.[70] Many Chinese Internet users therefore rely on Internet cafes for access to

---

[64] *See* OpenNet Initiative Bulletin 11 Analysis of China's Non-Commercial Web Site Registration Regulation, http://opennetinitiative.net/bulletins/011/#regreq (last visited Mar. 10, 2007) [hereinafter ONI Bulletin].

[65] By comparison, the average annual salary in China is $1,290 U.S. dollars. *See* Kara Spak, *China's Cell Phone Frenzy*, DAILY HERALD, Apr. 23, 2006, *available at* http://www.dailyherald.com/special/crossingchina/part2.asp.

[66] ONI Bulletin, *supra* note 64.

[67] *Id.*

[68] Mark Glazer, *Chinese Bloggers Run the Gauntlet of Forced Registration, Censorship*, U.S.C. ANNENBERG ONLINE JOURNALISM REVIEW, June 21, 2005, *available at* http://www.ojr.org/ojr/stories/050621glaser/. The registration requirement does not apply to blogs hosted on otherwise registered sites.

[69] ONI Bulletin, *supra* note 64.

[70] Jack Linchuan Qiu & Zhou Liuning, *Through the Prism of the Internet Cafe: Managing Access in an Ecology of Games*, 19 CHINA INFORMATION, 261, 265 (2005).

the web.[71] As of April 2006, there were approximately 113,800 Internet cafes operating in China.[72] This figure is down from earlier years, before a 2002 fire in an unlicensed Internet cafe killed twenty-four people.[73] In the wake of the fire, up to 45% of China's cafes were shut down,[74] and since 2003 authorities have adopted a policy of limiting licenses for new Internet cafes to a group of ten cafe franchisors.[75]

China regulates its Internet cafe industry heavily. In addition to setting the hours of operation, it bans children under sixteen from the cafes altogether and enforces strict zoning regulations that prevent cafes from operating within 200 meters of residential buildings and elementary and junior-high schools.[76] Internet cafes must keep records of their patrons' identities and the sites they visit and turn the records over on demand to the Public Security Bureau.[77] They are also required to use blocking software to prevent

[71] 29.5% of users surveyed in CNNIC's 18th Survey cited Internet cafes as their main locations for accessing the Internet. *See* CCNIC, *supra* note 1, at 11. In non-urban areas, the figure is reported to be around 80%. *See New Surveillance System for Shenzhen Province*, CHINACSR.COM, Mar. 23, 2006, http://www.chinacsr.com/2006/03/23/379-new-surveillance-system-for-shenzhen-Internet-cafes/. "PCs are sold at around 5,000 yuan (U.S.D 602.41) on average. By comparison, it costs only two yuan (24 cents) per hour, or even less during the night, to surf on the Internet in a café." *China's Internet Cafes Require Heed*, CHINA BUS. WEEKLY, May 18, 2004, http://www.chinadaily.com.cn/chinagate/doc/2004/05/18/content_331645.htm.

[72] Zhang, *supra* note 53.

[73] *Beijing Cafe Fire Kills 24*, Jun. 16, 2002, http://archives.cnn.com/2002/WORLD/asiapcf/east/06/15/beijing.fire/.

[74] *China overhauls Internet cafes*, XINHUA GENERAL NEWS SERVICE, Feb. 21, 2003, *available at* http://www.westlaw.com.

[75] Qiu & Liuning, *supra* note 69, at 280-282. For a list of the 10 café-franchisors, as well as a discussion of China's attempt to effectively nationalize the Internet-café industry, *see id.* at 283. For an indication that China may be ready to once again begin licensing independent cafes, *see Rumor China May Ease Limits on Internet Café Licenses*, CHINACSR.COM, Apr. 10, 2006, http://www.chinatechnews.com/2006/04/07/3870-rumor-china-may-ease-limits-on-Internet-cafe-licenses/.

[76] *See* ONI, INTERNET FILTERING, *supra* note 24, at 11-12.

[77] *Id.*

customers from accessing pornographic and other restricted websites.[78] Users who manage to circumvent these measures must be immediately disconnected from the Internet and reported to the local Culture Department.[79] Because failure to abide by these regulations may result in both civil and criminal liability,[80] many Internet cafes hire employees to monitor directly what's on their customers' screens.[81]

4. End-users

Obviously, the whole point of China's vast regulatory scheme is to control what its citizens can and cannot access on the Internet. Due to the state of existing filtering technology and the daily proliferation of potentially objectionable content on the Internet, it is functionally impossible to ensure that none of it makes it through the national firewall or past the official and de facto censors.[82] For this reason, China also resorts to blatant intimidation to discourage individual Internet users from attempting to access forbidden information in the first place.[83]

As we have already seen, Internet cafe users must register under their own identities and risk being reported to the Culture Department for accessing restricted websites.[84] In addition, ISP customers are required to register with their local police bureaus within thirty days of subscribing.[85] Nor is this an exercise in mere idle intimidation. China is rumored to have 35,000 "Internet police" dedicated to enforcing China's ever-expanding body of Internet regulations.[86] To illustrate just how serious a threat China

[78] *Id.*

[79] *Id.* at 17.

[80] *Id.*

[81] HUMAN RIGHTS WATCH, *supra* note 51, at 6.

[82] ONI, INTRODUCTION, *supra* note 11.

[83] Harwit & Clark, *supra* note 9, at 395.

[84] *See* ONI, INTERNET FILTERING, *supra* note 24, at 11-12.

[85] *Id.* at 10.

[86] *The Internet in China: A Tool for Freedom or Suppression?, J. Hearing Before the Subcomm. on Afr., Global Human Rights and Int'l Operations and the Subcomm. on Asia and the Pacific of the H. Comm. on*

believes the Internet to be, users accessing the Internet in at least one major city are now accompanied by interactive cartoon pop-ups of Internet police mascots "Jingjing" and "Chacha" as they surf the web. Hovering in the foreground at all times, the images serve as links to a website run by the Public Security Bureau where users can read available Internet regulations and even chat in real time with Internet police officers.[87] Radio Free Asia reported that its Chinese listeners were very intimidated by the pop-ups and believed them to be surveillance programs.[88]

All of this would border on the farcical were it not for the utterly draconian penalties facing users who violate these regulations. According to Amnesty International, Chinese authorities have imprisoned at least fifty-four people for Internet related activities deemed to be "subversive" or to "endanger state security."[89] Such activities include "signing online petitions, calling for reform and an end to corruption, planning to set up a pro democracy party, publishing 'rumors about SARS,' communicating with groups abroad, opposing the persecution of the Falun Gong, and calling for review of the 1989 [Tiananmen Square massacre]."[90] Documented sentences range from three to fifteen years.[91] Since January

International Relations, 109th Cong. 125 (2006) (testimony of Harry Wu, Publisher, China Information Center) [hereinafter Hearing]. While "Internet police" do exist in China, the exact number is unknown. *See* Rebecca MacKinnon, *Digital Silk Road Conference: The Internet in China*, RCONVERSTATION, http://rconversation.blogs.com/rconversation/2005/06/digital_silk_ro.html.

[87] Xiao Qiang, *Image of Internet Police: JingJing and Chacha Online*, CHINA DIGITAL TIMES, Jan. 22, 2006, http://chinadigitaltimes.net/2006/01/image_of_Internet_police_jingjing_and_chacha_online_hon.php.

[88] Hearing, *supra* note 86, at 172 (testimony of Libby Liu, President, Radio Free Asia).

[89] *Id.* at 205 (statement by T. Kumar, Advocay Director for Asia and the Pacific, Amensty International, U.S.A.).

[90] *Id.*

[91] *Id.* at 221 (statement by Ann Cooper, Executive Director, Comm. to Protect Journalists).

2001, it has been a capital crime to distribute state secrets over the Internet.[92]

In the sections that follow, the focus of this Note shifts from the nature and extent of China's control over its domestic networks and their connections to the outside world to the roles played by U.S. IT companies in both facilitating and perpetuating that control. The Note starts by outlining recent actions taken by these companies that have stoked the public's indignation and goes on to consider what, if anything, should be done to prevent them and others from engaging in such conduct again.

III. U.S. IT COMPANIES IN CHINA[93]

On January 25, 2006, Google unveiled Google.cn, a Chinese version of its popular search engine that censors what it determines to be politically sensitive results.[94] Google.cn was launched less than a month after Microsoft came under intense criticism from human rights activists for shutting down the blog of Chinese Internet journalist Zhao

[92] *Id.* at 211 (statement by T. Kumar, Advocacy Director for Asia and the Pacific, Amnesty International, U.S.A).

[93] The focus of this paper is on U.S. IT companies, which have garnered much of the international media attention and criticism. Among European IT companies, Telecom Italia and France Telecom have also cooperated with China's demands to censor Internet content. Reporters Without Borders, *European Parliament Condemns Ethical Breaches by Internet Sector Companies*, July 6, 2006, http://www.rsf.org/article.php3?id_article=18223. In response, the European Union Parliament has passed a resolution calling on the Council of Ministers and member States to develop a voluntary code of conduct regulating European IT companies doing business in Internet restricting countries. It also expressed its support for the Global Online Freedom Act of 2006, to be discussed *infra*. *European Parliament Resolution on Freedom of Expression on the Internet* (July 6, 2006), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2006-0324+0+DOC+XML+V0//EN&language=EN.

[94] A Google representative testified before the House Committee on International Relations that Chinese officials are not actively involved in determining what searches are censored. Hearing, *supra* note 86, at 96 (testimony of Elliot Schrage, Vice President for Corporate Communications and Public Affairs, Google, Inc.).

Jing. Zhao used his account on the Chinese version of Microsoft's MSN Spaces to call for a strike at a major Beijing newspaper when its editor was fired for reporting that as many as twenty villagers had been killed by police in clashes over land seizures.[95] Microsoft's decision to shut down Zhao's blog came approximately eight months after court documents revealed that Yahoo! had disclosed the identity of journalist Shi Tao, who was on trial for "illegally sending state secrets abroad."[96] Shi had used an email address from Yahoo! to expose a Chinese government directive instructing his newspaper on how to approach the upcoming fifteenth anniversary of the Tiananmen Square massacre.[97] As a consequence of Yahoo!'s decision to reveal his identity, Shi was sentenced to ten years in prison.[98]

The public outcry against these and other decisions by U.S. IT companies to assist China in censoring the Internet was swift and strong. Websites encouraging users to sign petitions, to terminate their Yahoo!, Google, or Microsoft email or blog accounts, and to seek alternative search engines immediately began to proliferate both within and without China.[99] In addition, a number of human rights organizations and Internet freedom and privacy watchdog groups began issuing reports documenting both the extent of

---

[95] Joshua Muldavin, Opinion, *In Rural China, A Time Bomb is Ticking*, INT'L HERALD TRIB., Jan. 1, 2006, at 6.

[96] Max Boot, Editorial, *Just Following Orders in China*, L.A. TIMES, Sept. 14, 2005, at B13.

[97] *Id.*

[98] *Id.* Subsequent investigations showed that Yahoo! revealed the identities of at least two other email users who were also sentenced to lengthy prison terms. Press Release, Reporters Without Borders, Yahoo! Implicated in Third Cyberdissident Trial: U.S. Company's Collaboration with Chinese Courts Highlighted in Jiang Lijun Case (Apr. 19, 2006), *available at* http://www.rsf.org/article.php3?id_article=17180 [hereinafter RWB Press Release].

[99] *See, e.g.*, BooYahoo!, http://www.booyahoo.blogspot.com/; Don't Be Evil, http://www.dontbeevil.com/. For a call by Beijing journalist and blogger Isaac Mao to boycott Microsoft, see Philip P. Pan, *The Great Firewall of China: Bloggers who Pursue Change Confront Fear*, WASH. POST, Feb. 21, 2006, at A1.

China's regulation of the Internet and the role U.S. companies played in facilitating it.[100] Even the federal government eventually got involved.

On February 14, 2006, the U.S. Department of State announced the creation of the Global Internet Freedom Task Force. [101] The Task Force's mission is to "maximize access to the Internet and help minimize government efforts to block information."[102] It will draw on the State Department's many resources to raise these concerns with other federal agencies, as well as private companies, NGOs, foreign governments, and international political organizations such as the UN.[103] The next day, the House Committee on International Relations held a joint hearing before the Subcommittee on Africa, Global Human Rights, and International Operations and the Subcommittee on Asia and the Pacific entitled "The Internet in China: A Tool for Freedom or Suppression?"[104]

A. What is to be Done?

While few U.S. IT companies would argue publicly that assisting China's speech censoring on the Internet or providing authorities with information that could lead to the long-term incarceration or execution of political dissidents is morally unobjectionable,[105] there is significant room for debate on what should be done about it. At one extreme, one could argue that the answer is nothing. Advocates of this view might argue that the acknowledged harm caused by the

[100] These groups included: Amnesty International, Human Rights Watch, Reporters Without Borders, and OpenNet Initiative.

[101] Josette Sheeran Shiner, Under Sec'y for Econ., Bus. & Agric. Affairs & Paula Dobriansky, Under Sec'y for Democracy & Global Affairs, Remarks on Global Internet Freedom (Feb. 14, 2006) (transcript available at http://www.state.gov/e/eeb/rls/rm/2006/61182.htm).

[102] *Id.*

[103] *Id.*

[104] *See* Hearing, *supra* note 86.

[105] Yahoo!'s representative, for example, testified that "we condemn the persecution of any person for exercising their right to free speech." *See* Hearing, *supra* note 86, at 99.

actions of U.S. IT companies in China is outweighed by the benefits deriving from their presence there. Alternately, they may favor this view because they are opposed in principle to any form of economic regulation. At the other extreme, one could argue that the answer is to prevent U.S. IT companies from doing business in China altogether. Such a policy could be defended on consequentialist or nonconsequentialist grounds, as well.[106] Between these two extremes, a case can be made for permitting U.S. IT companies to continue doing business in China, provided that they adhere to certain guidelines or restrictions. What these restrictions should be and who ought to enforce them will be matters for debate. Under one such view, the guidelines should be left for the IT industry or even the individual companies themselves to hammer out. Under another view, Congress ought to set the regulations. Under a third view, it will be a matter for multinational regulation.[107] We will consider each of these three main positions in turn.

---

[106] *See* discussion *infra* Parts 3.1.2, 3.1.2.1-2. We use the term "consequentialist" throughout in its technical or philosophical sense, according to which actions are to be judged on the basis of their effects. We use the term "nonconsequentialist" to refer to views on which actions are to be judged independently of those effects.

[107] Such a view might be emphasizing the need for self-regulation on the part of IT companies themselves, regardless of their places of incorporation. Since this merely highlights the fact that an industry might be international, it raises no new theoretical issues not implicated by our first version of the intermediate position and will not be considered on its own. On the other hand, such a view might be emphasizing the need for some form of *public* multinational regulation. Proponents of this view might be stressing the need for the United States to pressure other nations to regulate their domestic IT companies in a similar fashion. This view, however, is theoretically indistinguishable from our second version of the intermediate position and so will not be addressed independently here either. Alternately, these proponents might be advocating an appeal to international institutions like the World Trade Organization. This view *does* raise issues that are theoretically distinct from those implicated by our other versions of the intermediate position. Unfortunately, we lack the space required to do justice to them here. For an assessment of the case for challenging censorship in the WTO as a barrier to trade, see Tim

1. Maintaining the Status Quo

It was a constant refrain among the representatives of each of the IT companies testifying before the joint hearing that their presence in China is a net benefit to the citizens of the communist state.[108] Google, for example, insisted in its prepared testimony that if the company were required to abandon the Chinese market, local Internet users would be forced to rely on domestic search engines that are not likely to share Google's commitment to maximizing the accessibility of information[109] and, by implication, to taking a much more proactive approach to censoring search results.[110] Cisco, in turn, argued that if it were not permitted to sell its routers to China, local manufacturers would develop proprietary equipment incompatible with universal standards, thus resulting in a balkanization of the Internet that would further isolate Chinese users from the outside world.[111] Yahoo! and Microsoft emphasized the role the Internet played in spreading information about SARS.[112]

Although the developments we are discussing suggest that those in the IT sector who lobbied for the renewal of China's Most Favored Nation ("MFN") trading status in 1997 were overly optimistic when they claimed that the Internet would be an unequivocal force for liberalization in the

---

Wu, *The World Trade Law of Censorship and Internet Filtering*, 7 CHI J. INT'L L. 263 (2006).

[108] *See* Hearing, *supra* note 86, at 111; *see also id.* at 85 (Yahoo! asserting that "engagement is the better choice"); *id.* at 90 (Microsoft claiming "it is better for . . . United States Internet Companies to be engaged in China"); *id.* at 98 (Cisco insisting "our engagement is consistent with our Government's goals and it is a positive engagement"); *id.* at 66 (Google testifying that "we believe our decision to launch the Google.cn service . . . is a reasonable one, better for Chinese users and better for Google").

[109] *Id.* at 74.

[110] Google testified that it provides disclosure when search results are filtered. *Id.* at 66-67. It also emphasized the fact that Google.cn is available outside China, thus allowing interested parties to compare results from both its censored and uncensored search engines. *Id.* at 86.

[111] *Id.* at 112.

[112] *Id.* at 58, 64.

communist society,[113] even skeptics agree that it nevertheless offers citizens of totalitarian states one of their best opportunities for genuine exposure to the concepts of freedom and democracy.[114] The question here is whether this is a sufficient reason not to regulate how U.S. IT companies do business in China. To answer this we need to ask, first, whether the Internet in China really is any freer thanks to the presence of U.S. IT companies there and, second, whether efforts by U.S. authorities to regulate how these companies do business in China will effectively eliminate whatever benefits their presence may be determined to confer.

Google insists that Google.cn provides Chinese Internet users greater access to information than its domestic competitors.[115] In a statement submitted for the record to the Joint Hearing, Tom Malinowski of Human Rights Watch asks rhetorically how this could possibly be the case when both domestic and foreign IT companies are subject to the same regulatory regime.[116] In fact, tests conducted by the same group in May and August of 2006 revealed that Google.cn and a new Chinese search engine then being developed by Microsoft produced significantly more results on politically sensitive searches than Baidu, China's most popular domestic competitor.[117] At the same time, however, tests on Yahoo!'s Chinese search engine showed that it performed no better than Baidu.[118]

Human Rights Watch does not speculate on the reasons for the results. One possibility is that Google and Microsoft

[113] *Id.* at 112 (Testimony of Rep. Dana Rohrabacher (R-CA)).

[114] *See* Edgar Huang, *Flying Freely but in the Cage: An Empirical Study of Using Internet for the Democratic Development in China*, 8 INFO. TECH. FOR DEV., 145, 145-62 (1998). It is no small irony that freedom and democracy are two terms Microsoft censors in blog titles. *See* Kerry Howley, Op-Ed, *Freedom's Just Another Word: There are Many Ways Around the Great Firewall of China*, REASON ONLINE, June 21, 2005, http://www.reason.com/news/show/34053.html.

[115] *See* Hearing, *supra* note 86, at 66-67.

[116] *Id.* at 189.

[117] HUMAN RIGHTS WATCH, *supra* note 28, at 25.

[118] *Id.*

really are committed to resisting China's pressure to censor, because of an overarching commitment to the free flow of information.[119] Unfortunately, this interpretation seems to be at odds with Google's testimony before Congress, during which Google admitted that its license requires it to engage in self-censorship at Google.cn.[120] Rather than block only those results explicitly identified by Chinese authorities as objectionable, Google and other search engine operators are required to censor any content they judge to be in conflict with one of China's notoriously vague and open-ended laws and regulations.[121] Initially, this policy might appear to offer Google some leeway in interpreting those directives narrowly, in connection with the right to free speech enshrined in the Chinese constitution.[122] However, such a strategy, which could maximize the number of results its users can view, apparently has not occurred to Google.[123] Instead, Google testified that it determined what to censor by running searches on its competitors' engines and using its own engines to discover what sites had been blocked by the authorities at the server level.[124] If this is the case, then a better explanation for why its and Microsoft's searches yield more politically sensitive results than Yahoo!'s or Baidu's is not that either has a greater commitment to the free flow of information than these others, but rather that neither has been in the business of reading the minds of the government censors as long as their competitors have been.[125]

---

[119] Hearing, *supra* note 86, at 68 (Statement by Elliot Schrage).

[120] *Id.* at 95-96 (Testimony of Elliot Schrage).

[121] *Id.* at 96.

[122] Xian Fa art. 35, §1 (1982) (P.R.C.).

[123] Google testified that it did not know whether efforts were made to determine if the laws it is expected to follow in China are valid under the Chinese constitution or even if they are genuine laws to begin with. *See* Hearing, *supra* note 86, at 94-95.

[124] *Id.* at 96.

[125] It is interesting to note that Baidu itself was found to rely on the filters of its ISP to censor its search results rather than on its own. HUMAN RIGHTS WATCH, *supra* note 28, at 26.

It remains an open question whether Chinese Internet users are better off having access to search engines developed by U.S. IT companies, because only time will tell whether Google's and Microsoft's Chinese search engines will continue to offer access to a wider array of content than their domestic competitors, or whether, like Yahoo!'s, they will eventually become indistinguishable from them. A more convincing ground for concern is Cisco's contention that any attempt to regulate the sale of routers and other infrastructure-related hardware will provide an incentive for Chinese manufacturers to develop substitutes that fail to conform to universal standards in an effort to shield China's domestic networks from the global Internet.[126]

While facially plausible, Cisco's argument does not withstand closer scrutiny. The company acknowledges that the Chinese market for its products is very competitive.[127] Although Cisco curiously fails to discuss its own performance in China,[128] Chairman Smith indicated in his opening statements that Cisco holds sixty percent of the Chinese market for its products, accounting for approximately $500 million of the company's annual sales.[129] Contrary to what Cisco would have us believe, with U.S. IT companies currently competing in the market, Chinese competitors now have an incentive to develop proprietary routers and switches that would better facilitate the government's efforts to curtail its citizens' access to the global Internet, rather than compete for market share against Cisco's otherwise technologically superior products. If Cisco's market share were reduced or even eliminated by U.S. regulations, China's domestic server and router manufacturers would have less incentive to produce proprietary hardware that would simultaneously reduce their market shares abroad.

It is possible, of course, that Cisco is actually concerned about the prospect that Chinese authorities will decide to

[126] Hearing, *supra* note 86, at 90-91.

[127] *Id.* at 102.

[128] *Id.* at 79 (citing instead its worldwide sales figures).

[129] *Id.* at 3.

mandate the use of proprietary routers and switches instead. This would not be without precedent. In December of 2003, China announced that within six months all Wireless Local Area Network ("WLAN") equipment sold in the country would have to conform to its Wireless LAN Authentication and Privacy Infrastructure ("WAPI") encryption protocol rather than the current universal WLAN standard, or Wireless Fidelity ("Wi-Fi").[130]

The problem with this as an argument against U.S. regulation is twofold. First, Chinese authorities did not hesitate to impose these requirements on both domestic and foreign manufacturers. This suggests that if China were truly interested in creating proprietary standards for routers and other infrastructure-related hardware, it would do so immediately without waiting until its domestic manufacturers had a lion's share of the market.[131] Second, as Cisco itself points out, the U.S. government has been successful thus far in persuading China to postpone the policy's implementation.[132] Cisco offers no reason to presume that the U.S. would either lose its ability to influence China on such matters or impair its incentive to do so if Congress were to begin regulating the industry. On the contrary, it would probably only strengthen the U.S.'s initial bargaining position.

2. Imposing a Total Embargo

While there is some indication that most Chinese Internet users are better off due to the presence of U.S. IT companies

[130] Zia K. Cromer, *China's WAPI Policy: Security Measure or Trade Protectionism*, 2005 DUKE L. & TECH. REV. 0018, ¶ 3-7 (2005), *available at* http://www.law.duke.edu/journals/dltr/articles/PDF/2005DLTR0018.pdf.

[131] China's purported motive for developing its WAPI standard was perceived flaws in Wi-Fi's security features. *Id.* The fact that China is not presently pressing for a propriety standard for routers, servers, and switches suggests that it is satisfied with the security features available on standard models.

[132] Hearing, *supra* note 86, at 78. *See also* Richard Shim et al., *China, U.S. Strike Trade Accord*, Apr. 21, 2004, http://news.com.com/China,+U.S.+strike+trade+accord/2100-7351_3-5197087.html.

in China,[133] it does not necessarily follow that these companies should be free to cooperate with the Chinese authorities at their own discretion, or even that they should be permitted to work with them at all. We have already suggested that imposing some limitations on the ability of U.S. IT companies to censor content in China might generate greater benefits if it could be used as a bargaining chip in discussions over Internet policy with Chinese officials.[134] Taken to an extreme, this theory implies that Chinese Internet users would be best off if U.S. IT companies were prohibited from doing business in China altogether, at least until the government could be pressured into abandoning its commitment to censorship once and for all. Alternately, it might be argued that even if a total ban on the ability of U.S. IT companies to do business with China would not benefit the average Chinese Internet user most, it is nevertheless morally unacceptable to allow U.S. IT companies to collaborate with the Chinese government in depriving its citizens of their fundamental right to the freedom of expression. We will consider both these arguments briefly.

a. A Consequentialist Argument for a Total Embargo

Google testified before the Joint Hearing that it would reconsider its presence in China if it concludes that remaining there is inconsistent with its goals of maximizing global access to information.[135] However, few lawmakers or activists have come out in favor of a full and immediate embargo. Even Chairman Smith, who drew parallels between the actions of U.S. IT companies in China and IBM's collaboration with Nazi Germany during the Holocaust,[136] proposed legislation that would permit U.S. IT companies some leeway to continue doing business in

[133] *See* HUMAN RIGHTS WATCH, *supra* note 28, at 25.

[134] *See* discussion *supra* Part III(A)(1).

[135] Hearing, *supra* note 86, at 90.

[136] *Id.* at 5.

China.[137] Jonathan Zittrain, professor of Internet governance at Oxford and co-founder of Harvard Law School's Berkman Center for Internet and Society, has also come out against a complete ban.[138] He nevertheless maintains, "it's not a crazy position to say that these companies should not be there at all."[139]

It is far from clear that a complete embargo could be justified on consequentialist grounds. As we have already seen, there is some indication that Google.cn and Microsoft's new search engine provide greater access to politically sensitive websites than their Chinese competitors such as Baidu.[140] In order to show that Chinese Internet users would be even better off without access to these U.S. designed search engines and other IT products, defenders of a total ban must argue either that China's censorship policies would be less effective without American technology or that it would be more likely to abandon them sooner.

Neither of these scenarios is especially plausible. First, consider the suggestion that the success of China's ability to censor what its citizens can access on the Internet depends on its use of American technology. This does not seem to have hampered the administrators at Baidu.[141] Of course, Baidu appears to rely on filters at the ISP level to censor its users' searches.[142] Since Cisco dominates the Chinese market for infrastructure related equipment,[143] it is possible, therefore, that Baidu's success in censoring the information its users can access depends on its use of U.S. technology. Although a complete embargo would not deprive China of the use of U.S. technology it already possesses, it would prevent China from replacing the technology as it wears out or using it as the network expands. It would also prevent China from

---

[137] *See* Global Online Freedom Act, *supra* note 32.

[138] Tom Zeller Jr., *Internet Firms Facing Questions About Censoring Online Searches in China*, N.Y. TIMES, Feb. 15, 2006, at C3.

[139] *Id.*

[140] *See See* HUMAN RIGHTS WATCH, *supra* note 28, at 25-26.

[141] *Id.*

[142] *See supra* note 125.

[143] *See supra* note 129.

exploiting future innovations in the technology that might make filtering even more effective.

The strength of this argument depends on two rather dubious assumptions. The first is that Chinese manufacturers would not be able to create filtering technology comparable in quality to those of Cisco or its U.S. competitors. As we noted above, however, one of Cisco's chief arguments against regulation is that China's Internet would become even more insulated if it relied on domestic producers for its infrastructure-level hardware.[144] The second assumption is that even if China could not produce filtering technology as effective as that of its American competitors, it could not acquire comparable technology from Japanese, Korean, or other Western manufacturers instead.

This assumption is precisely the fatal flaw in the second scenario, in which China will abandon its censorship policy more quickly in the face of a comprehensive embargo. The idea that a unilateral embargo would hasten the demise of China's control over its domestic networks is decidedly optimistic. Like the previous scenario, it assumes that China would not be able to meet its demand for Internet related technology from domestic manufacturers or other foreign sources. This is unlikely. At the very least, any embargo with even a slight chance of success would require the support and cooperation of every nation with a major Internet hardware manufacturing industry. Given the strong incentives a sanctions regime would create both for cooperating parties to defect and for non-cooperating parties to increase production or serve as de facto middlemen,[145] a multilateral embargo would probably be only marginally more effective than a unilateral one.[146]

---

[144] *See* Hearing, *supra* note 86, at 90-91.

[145] Richard Posner, *Google in China*, The Becker-Posner Blog, Feb. 20, 2006, http://www.becker-posner-blog.com/archives/2006/02/google_in_china.html (applying the theory of cartels to economic sanctions regimes).

[146] Besides being much less likely given the size and importance of China's economy to world trade, a multilateral embargo is not a real possibility. *Id.*

b. A Nonconsequentialist Argument for a Total Embargo

If the foregoing argument is correct, a complete ban on the ability of U.S. IT companies to do business in China will not likely improve the average Chinese Internet user's ability to access politically sensitive content online. Any defense of such a ban, then, will have to be made on other grounds; one such possibility is that it is morally wrong to permit U.S. IT companies to engage in censorship of any kind. This would be a difficult case to make. It would mean, for example, that manufacturers could not assist authorities in blocking access to child pornography and other illegal content. But once we are willing to acknowledge that not all forms of censorship are bad, it becomes increasingly difficult to know just where to draw the line. There is, of course, a big difference between blocking access to child pornography and blocking access to politically sensitive sites like the BBC or Amnesty International. If, however, the Human Rights Watch study is accurate and Google's and Microsoft's Chinese search engines really do provide greater access to politically sensitive information,[147] then they are effectively reducing the amount of censorship that would otherwise exist. But if there is nothing intrinsically wrong with using censorship to begin with, then there ought to be nothing wrong with permitting it to be used when its net effect would be to decrease the amount of censorship that exists overall.

While there is reason to be skeptical that concerns about censorship alone could justify a total ban on the ability of U.S. IT companies to do business in China, the case for an embargo becomes much stronger when seen in light of examples such as Yahoo!'s complicity in the Shi Tao case.[148] It is no defense in cases like these that there will be less collaboration between U.S. companies and Chinese authorities than there would be between Chinese companies and Chinese authorities. In the first place, there is no indication that Yahoo! ever tried to resist disclosing Shi's

[147] *See* HUMAN RIGHTS WATCH, *supra* note 28.

[148] *See* Reporters Without Borders, *supra* note 93.

identity to the authorities. Instead, it appears to have promptly complied with what turns out to have been merely an informal request and not even a court order.[149] More importantly, however, there seems to be something inherently wrong with participating in the imprisonment of innocent people that cannot be outweighed on the grounds that, appearances to the contrary notwithstanding, U.S. IT companies will be less likely than their Chinese counterparts to disclose the identities of political dissidents.[150]

It would be morally outrageous to dismiss Yahoo!'s role in the imprisonment of Shi Tao and who knows how many others[151] as just part of the costs of doing business in China. It would be a callous insult to Shi and others like him to try to justify it as a necessary evil in the valiant effort by U.S. IT companies to bring freedom and democracy to the citizens of the communist state. At the same time, however, it would be a mistake to take it as grounds for justifying a complete embargo. Yahoo! ended up in the unfortunate position of having to disclose the identity of one of its users or potentially risk the imprisonment of its own employees[152] because it made the ill-considered decision to offer services in China that required it to collect sensitive information about its customers and to store that information on servers located in the country.[153] A company such as Cisco that sells only infrastructure-level hardware and does not interact with end-users like Shi would have no access to this kind of information in the first place.[154] Google made the decision not

[149] Hearing, *supra* note 86, at 5 (opening statements of Rep. Christopher H. Smith (R-NJ), Chairman, Subcomm. on Afr., Global Human Rights and Int'l Operations).

[150] Posner draws a similar distinction between the moral significance of censorship and surveillance as it pertains to the presence of U.S. IT companies in China. *See* Posner, *supra* note 145.

[151] At present count, Yahoo! has been implicated in at least two other cases. *See* RWB Press Release, *supra* note 98.

[152] Hearing, *supra* note 86, at 91 (testimony of Michael Callahan, Senior Vice President and General Counsel, Yahoo!, Inc.).

[153] Yahoo has since partnered with Alibaba.com and disavows operational control over its business there. *Id.* at 55-56.

[154] *Id.* at 100 (testimony of Mark Chandler).

to offer its Gmail or Blogger accounts in China precisely to avoid having to collect information of this nature.[155] Provided that a company does offer products or services that require it either to track the identities or activities of identifiable Internet users in China or to make this information available to the authorities, the troubling fact that other companies have done so is not a sufficient reason to prevent these companies from continuing to do business there. As long as it remains possible for U.S. IT companies to continue doing business in China without collaborating in the tracking and imprisoning of its Internet users, their continued presence in the country is at the very least morally defensible.[156]

3. Encouraging Self-Governance

Although Yahoo! came up short of admitting that it was ashamed of its involvement in Shi Tao's imprisonment, it did acknowledge being "very distressed" by it.[157] This leaves open the very urgent question of determining how best to prevent actions like this from occurring in the future.[158] One possibility is to rely on the companies to regulate themselves. A benefit of this is that it would obviate the need for the

---

[155] *Id.* at 76 (statement by Elliot Schrage). It does collect IP addresses, however. *Id.* at 241 (responses by Elliot Schrage to questions submitted for the record by Rep. Christopher H. Smith).

[156] Posner likewise suggests a middle ground on which U.S. IT companies would be permitted to continue doing business in China provided that they not participate in the surveillance of Chinese Internet users. *See* Posner, *supra* note 145.

[157] Hearing, *supra* note 86, at 99.

[158] Yahoo!'s response was to enter into a partnership with Alibaba.com, a leading Chinese e-commerce company, which now owns and operates Yahoo! China. Yahoo! retains a 40% ownership interest in Alibaba.com, as well as 35% voting rights. *Id.* at 179 (appendix). Critics of the arrangement maintain that Yahoo! entered into the partnership to maintain its stake in the Chinese Internet market while simultaneously achieving plausible deniability about Alibaba.com's day to day collaboration with Chinese authorities. *Id.* at 172 (testimony of Rep. Christopher H. Smith). Partnerships like these raise significant moral concerns that unfortunately lie outside the scope of this Note.

federal government to become involved. Due both to China's advent to the WTO in December 2001 and its PTNR trading status in the United States, any attempt by Congress to regulate the ability of U.S. IT companies to do business in China will raise serious legal concerns that could hold up the promulgation of regulations for years.[159] It would also serve to strain developing diplomatic relations between the two countries. China has one of the world's largest economies[160] and its influence over North Korea and other nations hostile to U.S. interests makes it an extremely valuable ally. Any approach to regulating the activities of U.S. IT companies in China that would not require the direct involvement of the federal government, therefore, ought to be seriously considered.

A further benefit of self-regulation is that it is more efficient than legislation.[161] It also imposes the cost of regulation on the corporations themselves. The real issue is its effectiveness. Despite Yahoo!'s self proclaimed "distress" at the fate of Shi Tao,[162] it doesn't take much of a cynic to wonder whether it would have felt the same way without the widespread public condemnation it suffered when it's involvement in the case was revealed. But perhaps this is unfair. Assuming for the sake of argument that a public outcry was necessary for the powers that be at Yahoo! to realize that something was wrong with willingly turning over the identities of its customers to Chinese authorities without so much as a court order,[163] the question is whether we can trust it and its competitors to voluntarily do the right

[159] Jill M. Brannelly, *The United States' Grant of Permanent Normal Trade Status to China: A Recipe for Tragedy or Transformation?*, 25 SUFFOLK TRANSNAT'L L. REV. 565, 576 (2002).

[160] Kieth Bradsher, *Economy*, N.Y. TIMES, Jan. 25, 2006, at C10.

[161] Earl A. Molander, *A Paradigm for Design, Promulgation and Enforcement of Ethical Codes*, 6 J. BUS. ETHICS 619, 621 (1987).

[162] Hearing, *supra* note 86, at 55 (testimony of Michael Callahan).

[163] *See* Posner, *supra* note 145. Yahoo admits not even inquiring as to the reasons for the request. *See also* Hearing, *supra* note 86, at 83-84 (testimony of Michael Callahan).

thing once their moral obligations have been laid entirely bare to them.

There is some evidence to support this. As noted above, when Google made the decision to enter China in the wake of the Shi Tao incident, it resolved not to make its email or blog services available to Chinese Internet users precisely because it wanted to avoid having to collect sensitive information about them.[164] In defending its actions in China, Google cites its corporate motto "Don't be evil" and insists that its approach to the country is fully consistent with this creed.[165] Whether this is entirely true is a matter for debate. As we have already noted, censorship is not necessarily morally objectionable.[166] Our main concern here, however, is not whether Google's conduct is morally defensible, but whether corporate mantras and codes like this are suitable substitutes for government regulation.[167]

a. Individual Codes of Conduct

The modern trend toward the adoption of corporate codes began in earnest during the second half of the twentieth century when a series of scandals embroiled the corporate world, leading to widespread calls for stricter regulation.[168] Studies indicate that by 2001, roughly three quarters of all

[164] *See* Posner, *supra* note 145.

[165] Hearing, *supra* note 86, at 70 (statement by Elliot Schrage).

[166] *See* discussion *supra* Part III(A)(2)(b).

[167] For a copy of Google's corporate code, entitled "Our Philosophy," *see* http://www.google.com/corporate/tenthings.html; Yahoo's "Code of Ethics" is available at http://yhoo.client.shareholder.com/governance/ethics.cfm; Microsoft's "Standards of Business Conduct" is available at http://www.microsoft.com/about/legal/buscond/; Cisco's "Code of Business Conduct" is available at http://investor.cisco.com/phoenix.zhtml?c=81192 &p=irol-govConduct.

[168] *See* Harvey L. Pitt & Karl A. Groskaufmanis, *Minimizing Corporate Civil and Criminal Liability: A Second Look at Corporate Codes of Conduct*, 78 Geo. L. J. 1559, 1574-98 (1990) (citing the antitrust tinged "Electrical Cases" of the 1960s, the Foreign Corrupt Practices Act of 1977, and the insider trading and defense contractor scandals of the 1980s as basic impetuses). *See also* George C. S. Benson, *Codes of Ethics*, 8 J. BUS. ETHICS 305, 306-07 (1989).

U.S. corporations had adopted written codes of conduct.[169] Despite this, their value has been the subject of continuing debate.

Critics have characterized codes as mere public relations tools and "window dressing."[170] They have emphasized their tendency to focus on curbing behavior thought to inhibit profitability rather than encouraging behavior believed to promote social responsibility.[171] After conducting empirical studies, critics have suggested that the adoption of codes has no impact on employee decision-making one way or the other.[172]

Proponents of corporate codes have, in turn, acknowledged their role as public relations tools.[173] They insist that a code can serve as a useful means of signaling to consumers that the corporation shares their ethical values, and that the public is sophisticated enough to know when the adoption of a code is just a cynical marketing ploy or bald attempt to deflect criticism.[174] Proponents of codes also point to more recent studies, which suggest that the codes have begun to reflect a greater concern about corporate citizenship and social responsibility.[175] Finally, proponents highlight

---

[169] Mark John Somers, *Ethical Codes of Conduct and Organizational Context: A Study of the Relationship Between Codes of Conduct, Employee Behavior and Organizational Values*, 30 J. BUS. ETHICS 185, 185 (2001). This number is likely only to increase with the enactment of the Sarbanes Oxley Act of 2002, section 406 of which requires companies to disclose whether they have a written code of conduct and, if not, to explain why not. Sarbanes Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (2002).

[170] Cecily A. Raiborn & Dinah Payne, *Corporate Codes of Conduct: A Collective Conscience and Continuum*, 9 J. BUS. ETHICS 879, 883 (1990).

[171] *See* Donald R. Cressey & Charles A. Moore, *Managerial Values and Corporate Codes of Ethics*, 25 CAL. MGMT. REV. 53 (1983).

[172] *See* Margaret Anne Cleek & Sherry Lynn Leonard, *Can Corporate Codes of Ethics Influence Behavior?*, 17 J. BUS. ETHICS 619, 627 (1998).

[173] Iain Munro, *Codes of Ethics: Some uses and abuses, in* CURRENT ISSUES IN BUSINESS ETHICS 97, 98 (Peter W. F. Davies, ed., 1997).

[174] *Id.*

[175] *See* Jang B. Singh, *A Comparison of the Contents of the Codes of Ethics of Canada's Largest Corporations in 1992 and 2003*, 64 J. BUS. ETHICS 17 (2006) (finding an increased concern with such issues as the

flaws in studies designed to show that codes have no impact on employee decision-making[176] and cite their own findings to the contrary.[177]

At the same time, however, even proponents of corporate codes acknowledge that the mere existence of a code is no guarantee that it will be effective.[178] Important factors that contribute to the strength of a corporate code's influence on employees include whether the code has the open support of senior management, its tone and readability, and its enforcement mechanisms.[179]

The very fact that the corporate code advocates acknowledge that their effectiveness depends on so many distinct variables is reason alone to doubt whether U.S. IT companies should be trusted to use them to set their own limits on doing business in China. Moreover, even assuming that a corporation manages to put an effective code of conduct in place, there will be tremendous pressure on it to relax its standards in the face of competition either from

environment among large Canadian firms). *See also* Somers, *supra* note 169, at 185 (arguing that "organizations that adopted formal codes of ethics exhibited value orientations that went beyond financial performance to include responsibility to the commonwealth.")

[176] *See* Cleek & Leonard, *supra* note 172. The study gauged the impact of codes of conduct on the decision-making behavior of employees by surveying the reactions to various scenarios of college students, only 32% of whom were working full time. The authors regarded the students as "fairly representative of the employees in most given organizations" because many have worked in entry-level positions before. *Id.* at 624. Cleek and Leonard acknowledge that their data suggests that full-time students were less equipped for ethical decision-making, but they nevertheless conclude that codes of ethics do not affect ethical decision-making. *Id.* at 627-28.

[177] Donald L. McCabe, Linda Klebe Trevino, & Kenneth D. Butterfield, *The Influence of Collegiate and Corporate Codes of Conduct on Ethics-Related Behavior in the Workplace*, 6 BUS. ETHICS Q. 461, 473 (1996) (finding that "there is a relation between corporate codes of ethics and employee behavior in the workplace, particularly to the degree that employees perceive the codes to be strongly implemented and embedded in the organizational culture.")

[178] Mark S. Schwartz, *Effective Corporate Codes of Ethics: Perceptions of Code Users*, 55 J. BUS. ETHICS 323, 325 (2004).

[179] *Id.* at 323.

firms without codes or from firms with codes that are less stringent or just poorly implemented.[180] This is especially true in the present context, because the potential benefits of cheating are especially high and the risks of detection are relatively low.

b. Industry-wide Codes of Conduct

One way to overcome at least some of the defects inherent to the code scheme would be to encourage the companies to adopt a uniform, industry-wide code of conduct. At the very least, this would eliminate the pressure to cheat that derives from competition from corporations with less demanding codes. It would also put pressure on firms without individual codes to adopt what had become, in effect, industry-wide standards. There would still be the risks associated with poor implementation, but these could be mitigated with an appropriate enforcement mechanism.

One initial concern with this approach is the potential difficulty of persuading a critical mass of companies within the industry to endorse a code of conduct that is sufficiently rigorous. Not every IT company is as vocal as Google about its social conscience, after all. It is likely to be enough here, however, that the adoption of an industry-wide code would be designed to forestall government intervention. If Congress is not satisfied with the terms of the code, it will set them itself. The threat of government regulation alone should ensure that less socially conscious industry members will not conspire among themselves to minimize the burden such a code would impose on them.

Of course, it is possible that the industry would be willing to gamble that its critics in Congress would not be able to muster enough support to enact particularly burdensome

[180] Skype, a European company that provides Voice over Internet Protocol ("VoIP") service and was recently acquired by Ebay, has been criticized for its so-called "peer pressure defense" of its decision to censor instant messages in China. John Leyden, *Skype Uses Peer Pressure Defense to Explain China Text Censorship*, THE REGISTER, Apr. 20, 2006, *available at* http://www.theregister.co.uk/2006/04/20/skype_china_censorship_row/.

legislation, whether for fear of alienating China or out of a more principled opposition to economic regulation in general. If this is a genuine worry, the industry could be pressured to include human rights activists and representatives of other concerned groups in the code drafting process. If it fails to do so, the public may infer that the industry does not take the moral hazards of doing business in China seriously. If it does include them, then either the activists will play a dominant role in the drafting process and we can be assured that the resulting code will be sufficiently rigorous, or they will not. If they do not play a dominant role in the process, they will nevertheless be able to report on the inner workings of the drafting committee and serve as restraints on members who would otherwise openly press for a minimally stringent code. While this is obviously not the ideal scenario, it is more likely to result in a superior code than if the drafting process occurred in a proverbial black box.

Three of the four companies in attendance at the 2006 Joint Hearing expressed an interest in working together to fashion industry-wide guidelines for conducting business in China.[181] They offered little by way of specifics, and even if their commitment is genuine, it is not altogether clear that self-regulation at the industry level is any better than at the corporate level. The main problem, not surprisingly, continues to be enforcement.

Industry-wide codes of conduct are especially susceptible to the "free-rider" problem.[182] Provided that enough companies adhere to the code to give it the appearance of

[181] Hearing, *supra* note 86, at 59, 64, 76 (Yahoo, Microsoft, and Google respectively). In fact, on February 1, 2006, Microsoft and Yahoo issued a joint statement to Congress's Human Rights Caucus expressing their concern about "recent developments in China." Press Release, Microsoft & Yahoo!, Inc., Microsoft and Yahoo! Inc. Joint Statement to U.S. Congress Human Rights Caucus on Policies Related to Access to Internet Content (Feb. 1, 2006) *available at* http://www.microsoft.com/presspass/legal/02-01MS-YahooStatement.mspx.

[182] Thomas A. Hemphill, *Self-Regulating Industry Behavior: Antitrust Limitations and Trade Association Codes of Conduct*, 11 J. BUS. ETHICS 915, 916 (1992).

industry-wide acceptance, individual signatories will have a strong incentive to cheat. But even a corporation that might otherwise resist the temptation to cheat would balk at providing a cloak of respectability to those it suspects of defecting. So unless there is some mechanism in place to monitor compliance and make cheating more costly than cooperating, few corporations will be willing to abide by even a moderately demanding industry-wide code for long.[183]

Monitoring and enforcement can be handled in at least three different ways. First, it can be left to industry itself.[184] This would require something along the lines of an industry trade association that possessed the power to impose fines or other penalties for noncompliance.[185] Historically, the courts have been skeptical of the use of such associations as tools of self-regulation, fearing their transformation into instruments of protectionism instead.[186] Nor is this concern entirely out of place here. It is conceivable, for example, that powerful members of the IT community may lobby for regulations that would require their competitors to incorporate those members' technology into any products or services they hoped to market in China. Such fears could be at least partially alleviated by the appointment of outside stakeholders to key positions on the monitoring committee.[187]

Second, to further safeguard the monitoring and enforcement process from manipulation by industry insiders, the monitoring could be entrusted to these independent stakeholders in its entirety. The Gap clothing retailer tried something like this with a distributor in El Salvador,

---

[183] The free-rider problem is typically used to illustrate a paradox about self-interest. Peter Asch & Gary A. Gigliotti, *The Free-Rider Paradox: Theory, Evidence, and Teaching*, J. ECON. EDUC. 33, 33 (1991). In fact, it is sufficient for the problem to arise that the signatories have reason to suspect each other of being self-interested. They need not actually be self-interested.

[184] *See* Hemphill, *supra* note 182, at 916.

[185] *Id.* at 917.

[186] *See* Ian Maitland, *The Limits of Business Self-Regulation*, 27 CAL. MGMT. REV. 132, 137 (1985).

[187] *See* Hemphill, *supra* note 182, at 918.

requiring the plant owner to permit a human rights group to monitor the work environment as a precondition to his receiving future orders.[188] The main problem with adopting this approach in the present context is the lack of an obvious enforcement mechanism. If the working conditions of The Gap's distributor in El Salvador failed to satisfy the independent observers, the plant owner would lose out on a lucrative contract. It is not clear what consequences a human rights group would impose on a U.S. IT company engaging in activities in China that contravened the envisioned code. To be sure, such a company would be the subject of a scathing report. But unless its authors are able to overcome traditional investor apathy[189] and a general lack of public concern about human rights abuses in China, it's unlikely that they would be able to impact these companies economically and, therefore, alter their behavior in any meaningful way.

Third, self-regulation can also be combined with governmental oversight.[190] Examples of this approach to the monitoring and enforcement of an industry-wide self regulatory scheme can be found in the securities and advertising industries, where independent rule making bodies such as the Investment Bankers Association and the National Advertising Review Board are combined with oversight by the Securities and Exchange Commission and the Federal Trade Commission respectively.[191] Proponents of such "mixed systems" argue that they are superior to both pure self regulation and complete government control

[188] Chris Seymour, *Independent Monitoring in El Salvador—Mandarin International Sweatshop Clothing Factory in San Salvador, El Salvador Negotiates with Industry Activist Charles Kernaghan*, THE PROGRESSIVE, Oct. 1996, at 13.

[189] Institutional investors have already begun to take notice. A group of 32 investment firms managing more than $22 billion U.S.D in assets submitted a statement to the 2006 Joint Hearing expressing its concern over the actions of U.S. IT companies in China and urging reform. *See* Hearing, *supra* note 86, at 226-27.

[190] Hemphill, *supra* note 182, at 916.

[191] *See* David A. Garvin, *Can Industry Self-Regulation Work?*, 25 CAL. MGMT. REV. 37, 47 (1983).

because governmental oversight reduces the risk that major industry participants will be able to subvert the process to their own advantage, while industry involvement ensures that the regulations will be sufficiently flexible so as not to inhibit efficient decision-making and the like.[192]

We have already discussed some of the additional advantages of self-regulation.[193] The adoption of a code of conduct, whether at the firm or industry level, can serve as a useful means of signaling to both employees and interested outsiders that the companies involved are committed to conducting business in ways that withstand moral scrutiny. Assuming that any attempt at industry self-regulation must be supplemented by appropriate legislation, what remains to be determined here is the form it should take. We will use the recently proposed "Global Online Freedom Act of 2006" as our point of departure for the discussion that follows.[194]

4. Government Regulation: The Global Online Freedom Act of 2006

The Global Online Freedom Act of 2006 ("Act") is a comprehensive bill designed to "promote freedom of expression on the Internet, to protect United States businesses from coercion to participate in repression by authoritarian foreign governments, and for other purposes."[195] Appealing to the rights of free speech and a free press, as well as to the right to communicate in all media and across all borders as guaranteed by Article 19 of the Universal Declaration of Human Rights,[196] the Act's drafters adopted a multi-pronged approach to the task of regulating how U.S. IT companies do business in countries like China. At the heart of the Act are a number of basic restrictions on the ability of U.S. IT companies to collaborate with these countries in limiting their citizens' access to the

[192] *See id.* at 49.

[193] *See* discussion *supra* Part III(A)(3).

[194] Global Online Freedom Act of 2006, H.R. 4780, 109th Cong. (2006).

[195] *Id.*

[196] *Id.* § 2.

Internet and tracking their online activities.[197] We will discuss the content of these restrictions at greater length below.

The Act would also establish the Office of Global Internet Freedom ("Office") in the Department of State.[198] The Office would "serve as the focal point for the interagency efforts to protect and promote freedom of electronic information abroad"[199] and spearhead the effort to "develop and implement a global strategy to combat state-sponsored and state-directed Internet jamming by authoritarian foreign governments, and the intimidation and persecution by such governments of their citizens who use the Internet."[200] Among others, it would also play a key role in implementing and overseeing the regulations imposed by the Act on U.S. IT companies and would work with them alongside human rights activists and academics to develop a voluntary industry-wide code of conduct.[201]

The Act would regulate the activities of U.S. IT companies doing business in designated "Internet-restricting countries." A list of Internet-restricting countries would be generated, on a yearly basis, by the President in consultation with the Office.[202] A country would be so designated if the President determines that its government "is directly or indirectly responsible for a systematic pattern of substantial restrictions on Internet freedom during the preceding one-year period."[203]

Under Title II of the Act, any U.S. IT company that operates a search engine or content hosting service in an

---

[197] *Id.* §§ 201, 202, 204, 206, 301.

[198] *Id.* § 104. There is no indication of how this would affect the newly established Global Internet Freedom Task Force. *See* Shiner, *supra* note 101.

[199] H.R. 4780, § 104(b)(1).

[200] *Id.* § 104(b)(2).

[201] *Id.* § 104(b)(6).

[202] *Id.* § 105(a).

[203] *Id.* § 105(a)(2). *See also id.* at § 105(a)(3)(B) (mandating that initial designees shall include Burma, China, Iran, North Korea, Tunisia, Uzbekistan, and Vietnam).

Internet-restricting country would be forbidden from storing any data related to those products on computer hardware located there.[204] In addition, search engine operators would be forbidden from using certain "protected filter terms"[205] to limit search results,[206] while companies providing hosting services would be prohibited from blocking access to U.S.-supported websites or content,[207] including any created by the Voice of America or Radio Free Asia.[208] Companies that use filter terms or block access to websites or content not explicitly protected under the Act would be required to disclose that information to the Office.[209]

Under section 206(a), providers of content hosting services would be strictly forbidden from disclosing the identities of their users to officials of Internet-restricting countries except for legitimate law enforcement purposes.[210] Section 3(8)(B) stipulates that such purposes do not include "the control, suppression, or punishment of peaceful expression of political or religious opinion, which is protected by Article 19 of the International Covenant on Civil and Political Rights."[211] Section 206(b) provides a private right of action for any person harmed by the improper disclosure of personal information to an Internet-restricting country, regardless of citizenship or amount in controversy.[212]

---

[204] *Id.* § 201.

[205] "Protected filter terms" would be identified by the Office. *Id.* § 104(b)(4)(A). They would include "key words, terms, and phrases relating to human rights, democracy, religious free exercise, and peaceful political dissent, both in general and as specifically related to the particular context and circumstances of each Internet-restricting country . . . ." *Id.*

[206] *Id.* § 202(b).

[207] *Id.* § 204.

[208] *Id.* § 102(2). Other examples of U.S.-supported content cited in that section include the Annual Country Reports on Human Rights Practices and the International Religious Freedom Reports. *Id.*

[209] *Id.* §§ 203, 205.

[210] *Id.* § 206.

[211] *Id.* § 3(8)(B).

[212] *Id.* § 206(b).

Section 207 establishes civil and criminal penalties for violations of various provisions of the Act.[213] Companies that provide personal data to officials of Internet-restricting companies in violation of section 206(a) would be subject to civil penalties of up to $2,000,000.[214] Officers, directors, employees, agents, and participating stockholders of companies who willfully violate or attempt to violate section 206(a) would be subject to fines of up to $100,000 and/or five years in prison.[215] Fines for violations of sections 201-205 would not exceed $10,000 for corporations[216] or natural persons,[217] and the latter would face imprisonment for up to one year.[218]

Other provisions would amend the reporting requirements of the Foreign Assistance Act to include assessments of a potential aid recipient's commitment to the freedom of electronic information[219] and require the President to make annual reports on U.S. efforts to counter attempts by Internet-restricting countries to limit their citizens' online freedoms.[220] In addition, Title III of the Act would impose licensing requirements and other restrictions on companies seeking to export equipment that would be used for censorship purposes to Internet-restricting countries.[221]

a. Assessment

The Act's drafters did an admirable job in many respects. By preventing U.S. IT companies from storing sensitive user information in Internet-restricting countries and imposing hefty fines and possible prison sentences on corporations for

[213] *Id.* § 207.
[214] *Id.* § 207(a)(1).
[215] *Id.* § 207(b)(1).
[216] *Id.* § 207(a)(2).
[217] *Id.* § 207(b)(2).
[218] *Id.*
[219] *Id.* §§ 103, 301.
[220] *Id.* § 105(b)(1)(C).
[221] *Id.* § 301.

improperly disclosing that information to those countries, the Act might prevent the kind of sickening collaboration seen in the Shi Tao case from occurring in the future or, at the very least, might ensure that the companies involved would be held accountable.[222] Because the Act defines "United States Business" to include foreign subsidiaries of U.S. companies in which they have a controlling interest,[223] it would also ensure that Yahoo! and others tempted by its example would not be able to escape liability under section 207 by partnering with domestic Chinese Internet companies in a thinly veiled attempt to achieve some form of plausible deniability.[224]

The Act would also bring a much-needed element of flexibility to the regulations. This would be achieved both by encouraging industry involvement in the development of a voluntary code of conduct and by requiring the President to

---

[222] *See* Neal J. Conley, Comment, *The Chinese Communist Party's New Comrade: Yahoo's Collaboration with the Chinese Government in Jailing a Chinese Journalist and Yahoo's Possible Liability Under the Alien Tort Claims Act*, 111 PENN. ST. L. REV. 171 (2006) for a cautiously optimistic assessment of the possibility that Shi Tao and others like him might prevail against Yahoo under the Alien Tort Claims Act.

[223] H.R. 4780, § 3(11)(C)(i). The ability of Congress to provide for extraterritorial application of its laws to U.S. citizens abroad has long been recognized by the courts. *See* Blackmer v. United States, 284 U.S. 421, 437 (1932) ("While the legislation of the Congress, unless the contrary intent appears, is construed to apply only within the territorial jurisdiction of the United States, the question of its application, so far as citizens of the United States in foreign countries are concerned, is one of construction, not of legislative power."). But under the "control theory" of corporate nationality, foreign corporations controlled by U.S. citizens would themselves be subject to U.S. law under the principle articulated in *Blackmer*. *See* William Laurence Craig, *Application of the* Trading with the Enemy Act *to Foreign Corporations Owned by Americans: Reflections on* Fruehauf v. Massardy, 83 HARV. L. REV. 579, 589 (1970). Even in cases where the subsidiary cannot be reached, however, the controlling corporation can still be held liable for the actions of a foreign subsidiary. *See* H. Lowell Brown, *Parent-Subsidiary Liability Under the Foreign Corrupt Practices Act*, 50 BAYLOR L. REV. 1, 2 (1998) (pointing out that U.S. parent corporations are subject to liability under the Act for violations committed by foreign subsidiaries immune from prosecution).

[224] *See* Brannelly, *supra* note 159.

reevaluate the status of designated Internet-restricting countries on an annual basis. This flexibility is also evident in the prospective role to be played by the Office of Global Internet Freedom. Not only would it be given the authority to recognize protected filter terms, for example, but it would also be specifically authorized to do so in light of the particular social and political contexts of each of the Internet-restricting countries.[225]

That being said, the Act is vulnerable to criticism on a number of fronts. Take the provisions preventing companies from using protected terms to filter search results or blocking U.S.-supported content. The upshot of these provisions is that U.S. IT companies would be prohibited from filtering or blocking much of the content Chinese officials are likely to want to censor. Because this content can be blocked at the ISP or server level as well, it is possible that these provisions would not be deal-breakers from China's point of view. But if this is the case, then it is not clear why U.S. IT companies should be prevented from cooperating in the first place. As we argued above, this form of censorship is not necessarily objectionable. An alternative might be to require U.S. IT companies to disclose to users the terms being filtered or the content being blocked. Instead of relying on the possibility that the protected content will somehow make it through the firewall for users to see, this solution would at least give users the opportunity to learn what the government is preventing them from seeing. Of course, this presupposes that Chinese authorities would permit the practice.[226] If not, it might still be desirable

[225] H.R. 4780, § 104(b)(4)(A).

[226] It is not altogether clear that such a requirement would be especially objectionable to the authorities. Few totalitarian societies celebrate the freedom of information. Instead, they extol the virtues of censorship by proudly proclaiming its value in protecting the vulnerable among them from the corrupting influences of outsiders. It is unlikely that such disclosure would be seen as the kind of embarrassment it would be in our own society. It might even be thought to serve a useful intimidation function. *See* discussion *supra* Part II(C)(4). If users know the government is censoring results for certain search queries, they might be less inclined to run them. Whether such a possibility should test our

to require them to disclose and publish the information outside of China.

There is a potential First Amendment issue lurking here, as well. The Supreme Court in *West Virginia State Bd. of Educ. v. Barnette* held that the Constitution protects not just the freedom to speak, but also the freedom not to speak.[227] By forbidding search engine operators from censoring certain politically sensitive search results and, thereby, compelling them to display these results on their servers, the Act would arguably violate this right.

We will assume for the sake of argument that search results constitute speech for First Amendment purposes.[228] It is a further question whether a requirement compelling search engines to include certain results and, therefore, "speak" is for that reason unconstitutional. The Supreme Court distinguishes broadly between political and

---

faith in the value of a disclosure requirement, of course, is something to bear in mind.

[227] West Virginia State Bd. of Educ. v. Barnette, 319 U.S. 624, 645 (1943).

[228] An argument might be made that the Act regulates conduct, not speech. After all, it would simply prevent IT companies from using filtering software in Internet restricting countries. But, conduct is only protected under the First Amendment if it is expressive. United States v. O'Brien, 391 U.S. 367, 385 (1968) ("The statute attacked in the instant case has no such inevitable unconstitutional effect, since the destruction of Selective Service certificates is in no respect inevitably or necessarily expressive. Accordingly, the statute itself is constitutional."). Since the companies subject to the Act make the content they censor in China freely available to users in other countries, they would be hard-pressed to make the case that their conduct in China is expressive. The problem with this argument is that the Supreme Court has since acknowledged that forcing parties to send e-mails or post announcements on bulletin boards is a form of compelled speech that implicates the First Amendment. Rumsfeld v. Forum for Academic & Institutional Rights, Inc., 126 S. Ct. 1297, 1307 (2006). But including links to certain politically sensitive content on a search result page has more in common with sending an e-mail or posting a flier than with damaging a draft card or holding a door open for a military recruiter. Since a decent argument can be made that the Act regulates speech, and since this would pose a tougher test case for determining its constitutionality anyway, we will leave the argument in this Note to one side.

commercial speech, affording the government greater leeway in regulating the latter. In evaluating this objection, therefore, we first need to determine the class of speech being implicated here.

The Court's commercial speech jurisprudence dates back to 1942, when it held that the "Constitution imposes no such restraint on government as respects purely commercial advertising."[229] Later cases have taken this holding to cover speech that "did no more than propose a commercial transaction."[230] While the decisions of companies like Google, Yahoo!, and Microsoft to censor search results in China are almost certainly commercially rather than politically motivated,[231] it would be rather difficult to shoehorn them into the narrow meaning of "commercial speech" adopted by the Court. Although a promise to engage in censorship may have been an essential part of their proposals for a commercial transaction with China, the filtering they are engaging in pursuant to the terms of the resulting agreement is in no way the same as a mere advertisement or proposal. Even assuming that it "advertises" their willingness to continue the relationship or to engage in like transactions with other repressive regimes, it does more than this—it prevents users from searching the Internet using filtered terms. Nor is this just a semantic quibble. Members of the Court in recent years have signaled a general dissatisfaction with the theoretical soundness of the distinction between commercial and political speech,[232] as well as dissatisfaction with the application of less than strict

[229] Valentine v. Chrestensen, 316 U.S. 52, 54 (1942).

[230] Pittsburgh Press Co. v. Pittsburgh Committee on Human Relations, 413 U.S. 376, 385 (1973).

[231] This notwithstanding Google's insistence before Congress that it was motivated by a corporate commitment to maximizing access to information world-wide. *See* Hearing, *supra* note 86.

[232] Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 581 (1980) (Stevens, J. concurring) (lamenting the "blurry line" the Court draws between commercial and noncommercial speech).

scrutiny to attempts to regulate the former.[233] In this climate, the Court is unlikely to adopt the broader conception of commercial speech needed for the doctrine to apply in the present context.

Whatever difficulty we may have in viewing the Act as implicating noncommercial speech no doubt derives in large part from an inability to see anything but an economic motive underlying the actions it is designed to regulate. As Justice Stevens has observed, however, "the economic motivation of a speaker [should not] qualify his constitutional protection; even Shakespeare may have been motivated by the prospect of pecuniary reward."[234] What matters is the content of the speech, and many of the search terms the Act would protect are overtly political in nature.

If motive is irrelevant, that Act might be challenged under the rationale of *Wooley v. Maynard*, which held that states cannot compel their citizens to "use their private property as a "mobile billboard" for [their] ideological message[s]."[235] Of course, the Plaintiffs in *Wooley* were Jehovah's Witnesses who explicitly objected to the message they were being compelled to convey. Here, the only people being forced to "speak" are companies that make the same content freely available to their users outside of China. This fact would presumably undermine any claim that they might have to find the policy objectionable on non-commercial grounds. It is probably enough under *Wooley*, however, that they simply object to being compelled to express an ideology in a public forum, even if they agree with it in private. At the very least, this would be consistent with the sentiment

[233] 44 Liquormart v. R.I., 517 U.S. 484, 517 (1996) (Scalia, J. concurring) (echoing Justice Thomas's view that the Court's commercial speech jurisprudence has "nothing more than policy intuition to support it," though coming short of calling for its outright rejection). Only four of the Justices joined in the part of the opinion endorsing the Court's application of its traditional four-part test for evaluating restrictions on commercial speech, which applies intermediate scrutiny. *Id.* at 1506-07.

[234] Central Hudson, 447 U.S. at 580 (Stevens, J. concurring).

[235] Wooley v. Maynard, 430 U.S. 705, 715 (1977) (holding a New Hampshire law that effectively required motorists to display the state's "Live Free or Die" motto unconstitutional).

quoted above, which says nothing about having to find the content of the message one is forced to display disagreeable.

Even if our reading of *Wooley* is correct, it does not necessarily follow that the Court would find the Act unconstitutional. In fact, there is good reason to think otherwise. The Court in *Pruneyard Shopping Center v. Robins*[236] and, more recently, in *Rumsfield v. Forum for Academic and Institutional Rights* (*"FAIR"*)[237] has implied that institutions serving the public can be compelled to permit their facilities to be used for speech with which they disagree when it is unlikely that they will be taken as endorsing it. But it is highly unlikely that even a casual Internet user would believe that search engines endorse the content of the millions of websites they make accessible in many common queries. Of course, the law schools in *FAIR* had the option of avoiding the requirement to accommodate military recruiters by refusing to accept federal funds,[238] but the IT companies in the present context could just as easily avoid the application of the Act by declining to do business in Internet restricting countries.

Any lingering doubt as to how the Court would receive such a case would seem to be laid to rest decisively in *FAIR*. There, the Court went so far as to assert that by citing *Barnette* and *Wooley* in objection to a policy requiring law schools to email students about military recruiters when they were already doing the same for others, the Plaintiffs

[236] Pruneyard Shopping Ctr. v. Robins, 447 U.S. 74, 100 (1980) (upholding a state law requiring shopping centers to permit third parties to distribute political leaflets on their premises and rejecting a Wooley claim on the grounds that no one would take the center to be endorsing the flyers being distributed in its parking lots).

[237] Rumsfeld v. Forum for Academic & Institutional Rights, Inc., 126 S. Ct. 1297, 1310 (2006) (upholding a law withholding federal funds from law schools that prohibit military recruiters on campus and observing that the law does not require the schools to speak and permits them to dissociate themselves from the message through protests and other outlets).

[238] *Id.* at 1303.

were "trivializ[ing] the freedom protected in [those cases].[239] But, including results for protected terms is even easier than sending email. All it requires is that search engine operators refrain from filtering them out in the first place. An IT company would be ill-advised to bring a case under *Barnette* and *Wooley* in the present context, where a genuine political objection to the requirement is even less likely to be forthcoming. If the Court thought the plaintiffs were trivializing these freedoms in FAIR, it is likely to find them to be outright mocking them here.

Perhaps the biggest problem with the Act is Section 201's wholesale restriction on the ability of search engine operators and content hosting service providers to store any information on computer hardware located within Internet-restricting countries. The difficulty with this is that China's national firewall makes accessing and using websites housed on servers located outside the country prohibitively slow. As Google testified at the 2006 Joint Hearing, this was one of the principal factors influencing the company's decision to develop a Chinese version of its search engine in the first place. While it is absolutely essential that U.S. IT companies be prohibited from storing personal information about its users within Internet-restricting countries, it is also important that they be able to provide users with products and services that work at least as well as their competitors'. This requires that they be able to store at least some data within these countries. Industry representatives could work alongside the Office of Global Internet Freedom to determine how best to balance these two considerations.

IV. IN DEFENSE OF A HYBRID SOLUTION

Whatever response we ultimately adopt here will have varying economic and political significance for people and governments the world over. For the most part, however, the debate has been framed as a contest between the

[239] *Id.* at 1308 (arguing both that such speech is only incidental to the requirement to accommodate military recruiters and that it has little in common with a "government-mandated pledge or motto.").

economic interests of the IT companies and the political interests of the Chinese people. This approach ignores not just the economic interests of the Chinese people and the political interests of the IT companies, but any of the competing interests of all those groups not a part of this equation, including the American people. This is not to say, of course, that we need to carefully and impartially balance all these competing interests in some grand utilitarian calculus before deciding what to do. But it does suggest the need for a criterion for determining whose interests matter and to what extent, and it is precisely this that has been missing from the present debate.

The answers to these questions will depend largely on the nature of the approach to regulation. The interests considered by the government when it acts do not necessarily overlap with those that a corporation has an obligation to promote. As we argued above, however, it is the very nature of a corporation's interests that make a purely self-regulatory response untenable from a practical point of view.[240] For that reason, we have suggested that it would have to be supplemented by appropriate legislation. We implied that the positive effect a properly implemented corporate code is likely to have on a firm's moral and legal culture is sufficient reason to retain it despite the possibility of replacing it altogether with a purely legislative regulatory regime. We will argue now that there is a deeper theoretical reason for preferring a hybrid regime of this sort—a reason grounded in a conceptual limitation common to most contemporary views on the nature of the State and the interests to which it is beholden.

A. The Nature of the State in Contemporary Political Theory

The precise nature of the kinds of interests a government is obliged to promote differ, of course, depending on the theory of the State being used. Within contemporary Anglo-American political thought, these theories typically assume

[240] *See supra* Part III(A)(3).

one of three broad types: libertarian, liberal, and communitarian. According to one popular strand of libertarianism, the purpose of the state is to safeguard the acquisition and transfer of private property.[241] According to Rawlsian-style liberalism, it is the government's duty to distribute the benefits and burdens of citizenship in such a way as to make the least well-off better off than they would be under any alternative distribution.[242] According to communitarians, the moral authority of the state cannot be reduced to an actual or hypothetical contract between free and independent individuals. Instead, individuals and their norms of governance are products of the traditions and values of the communities from which they emerged and to which they are ultimately beholden.[243]

For the purpose of the present argument, however, it is largely irrelevant which of these views we ultimately adopt. Despite their numerous and often polarizing differences, all three share a common core assumption: a State's principal obligations are to its citizens.[244] But because the benefits of the proposed legislation would seemingly accrue primarily to the citizens of China and other Internet restricting countries, while most of the costs would be borne by U.S. IT companies and their domestic and foreign investors, it is difficult to see how the adoption of something like the Global Online Freedom Act could be justified within the framework of any of the standard conceptions of the State outlined above.

One possibility is that government regulation is likely to have long term benefits for U.S. citizens that would outweigh

---

[241] *See* ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA 26-29, 149 (1974).

[242] JOHN RAWLS, A THEORY OF JUSTICE 75 (1971).

[243] *See* MICHAEL J. SANDEL, LIBERALISM AND THE LIMITS OF JUSTICE 14, 173-174 (1982).

[244] This is explicit in libertarianism, as well in Rawls's view. LINDA BOSNIAK, THE CITIZEN AND THE ALIEN: DILEMMAS OF CONTEMPORARY MEMBERSHIP 6 (2006). The priority afforded citizens, or members of the community, over outsiders is especially pronounced in communitarianism. David Morrice, *The Liberal-Communitarian Debate in Contemporary Political Philosophy and its Significance for International Relations*, 26 REV. OF INT'L STUDIES 233, 243 (2000).

these immediate costs. This might be the case, for example, if it were to hasten the demise of Communist rule in China and bring about closer and more profitable political and economic ties between the two countries. As we argued above, however, this is a dubious assumption.[245]

The drafters of the Act appealed instead to a general policy of ensuring that the Internet remains a forum for the free and open flow of information and ideas.[246] Moreover, having ready access to information that an uncensored Internet affords is obviously of great benefit to everyone worldwide. It would follow, therefore, that the Act does indeed promote the interests of U.S. citizens after all. The problem with this argument, however, is that the Act does little if anything to protect or increase the access to information U.S. citizens already enjoy. Instead, it would merely extend that freedom to citizens of those countries who do not presently possess it. This is undeniably a laudable goal. Unfortunately, it would be difficult to justify on any of the competing theories of the State we have mentioned.

One further possibility is that there is symbolic value in the U.S.'s preventing its IT companies from collaborating with Internet restricting regimes to prevent over 1/6 of the world's population from enjoying the same uncensored access to information that its own citizens take for granted. On this view, the Act would signal to the rest of the world that the U.S. is serious about its commitments to the freedoms it espouses and would generate international goodwill among both citizens of these countries, who may one day come to power and return the favor, as well as to third party observers. At any rate, something like this seems to be implicit in the drafters' understanding of the Act.[247]

While prima facie plausible, this argument is vulnerable to attack on a number of points. First, there is reason to believe, as mentioned above, that search engines operated in China by U.S. IT companies frequently provide greater

[245] *See supra* Part III(A)(2)(a).

[246] Global Online Freedom Act of 2006, H.R. 4780, 109th Cong. § 101(1) (2006).

[247] *See id.* § 101(3).

access to content than those offered by their Chinese competitors. But if this is the case, then any action on the part of the U.S. that limits their ability to business in China would amount to a pyrrhic victory for the proponents of the freedom of information, elevating symbolism over substance.

Second, the concept of "international goodwill" is so vague that it could be used to justify any action that might find even a modicum of support abroad. But, this would effectively undermine the normative restraints on State action recognized by the standard political theories. Moreover, there is good reason to think that if there is such a thing as "international goodwill," it would be better achieved by working within the institutional framework already established for dealing with these kinds of disputes, such as the Organization of Economic Cooperation and Development, the World Trade Organization, the United Nations World Summit on the Information Society, and the Internet Governance Forum.[248] This is especially true in a geo-political environment that is becoming increasingly suspicious of what it takes to be U.S. unilateralism of any stripe.[249]

While we have failed to discover an interest sufficient within the conceptual limitations of contemporary mainstream political thought to warrant government regulation of the type envisioned by the sponsors of the Global Online Freedom Act, the case for the necessity of corporate self-regulation is not so bleak. Current theoretical accounts of the nature and obligations of the corporation are adequate to accommodate it. Additionally, they provide an indirect way of justifying government action as well.

[248] In fact, the drafters of the Act encourage the President to do just that. *Id.* § 102(1).

[249] *See, e.g.*, UNILATERALISM AND U.S. FOREIGN POLICY: INTERNATIONAL PERSPECTIVES 1-4, 19-35, (David M. Malone & Yuen Foong Khong, eds., 2003).

B. The Nature of the Corporation: Stockholders v. Stakeholders

The dominant theoretical view of the nature and duties of the corporation is probably the one articulated by Milton Friedman in his influential polemic, "The Social Responsibility of Business is to Increase its Profits."[250] On this view, a corporation's one and only duty is to maximize returns on its stockholders' investments. Any attempt by management to subordinate this interest to some other socially desirable outcome constitutes a breach of its fiduciary duties to the corporation's owners. The only exception to this duty is that stockholder interests cannot be pursued through fraud or deceit.

Critics of Friedman's view have responded with the increasingly influential alternative dubbed by R. Edward Freeman the "stakeholder theory of the firm."[251] On this view, a corporation has obligations not just to its stockholders, but to everyone with a stake in the activities of the firm, including employees, management, suppliers, customers, and members of the communities in which they do business. A number of states have acknowledged the legitimacy of the stakeholder theory by adopting so-called "constituency statutes," which explicitly permit corporations to consider the possible effects of their proposed actions on such stakeholders in the decision-making process.[252]

We lack the space here to weigh the relative merits of these two positions in anything approaching sufficient detail.[253] Assuming that something like Freeman's

---

[250] Milton Friedman, *The Social Responsibility of Business is to Increase its Profits*, N.Y. TIMES, Sept. 13, 1970, at SM17.

[251] R. Edward Freeman, *A Stakeholder Theory of the Modern Corporation*, *in* THE CORPORATION AND ITS STAKEHOLDERS: CLASSIC AND CONTEMPORARY READINGS 125, 126 (Max B.E. Clarkson ed., 1998).

[252] *See, e.g.*, NY BUS. CORP. § 717(b).

[253] Suffice it to say that Friedman's view seems to entail the implausible consequence that individuals doing business in their own capacity can escape moral scrutiny for the effects of their actions on "other constituencies" by entrusting their money instead to corporate agents, who would be free to do their dirty work with relative impunity under the

stakeholder theory is at least conceptually coherent, however, we can proceed to develop in fairly short order the outlines of the theoretical defense of government regulation in the present context that no mainstream account of the nature of the modern state seemed capable of providing.

C. From Self-Regulation to Legislation

The argument itself is fairly straightforward. If corporations have a duty to consider the effects of their actions on stakeholders, and stakeholders include their customers and the members of the communities in which they do business, then large transnational corporations will have duties to the citizens of all the countries in which they operate. Frequently, however, meeting their duties to these stakeholders puts corporations at a competitive disadvantage vis-à-vis their competitors. It is in their interest, therefore, to encourage industry-wide compliance with these duties through the adoption of a uniform code of conduct. The problem with this is that in the absence of an oversight mechanism possessing the authority to compel their compliance, individual firms will often find it to their advantage to cheat. But none of the firms will trust each other enough to vest any one of them with the capacity to police the agreement. An outside party powerful enough to stand up to pressure from even the largest corporation is therefore needed to assume this role. The only entity fitting this description is the federal government. And because the state would be acting in the direct interest of corporations formed under its own laws this time around, the limitations on State action imposed by the orthodoxies of contemporary

auspices of their fiduciary responsibilities. Freeman's view, on the other hand, vests management with considerably more power over shareholder assets than Friedman's and may threaten the ability of corporations to raise capital as a result. It seems unlikely, however, that managers would abuse this greater discretion under the stakeholder theory to the extent that potential stockholders would consider it unprofitable to invest.

political theory would pose no bar to the required legislation.[254]

There is much that would need to be developed in this view, as well as much that it cannot do. It would be necessary, for example, to address such issues as the nature and extent of a corporation's obligations to its foreign stakeholders. In particular, we would need to address whether those obligations are determined by the norms of the host country or those of the country of incorporation. This is especially important in cases where most if not all of the employees and managers on the ground will be from the local population. We will also need to determine what to do in cases where the industry fails to recognize its obligations to these other stakeholders and does not individually appeal to the government for aid in developing and enforcing a corporate code. Any attempt to impose a code on an industry from without and to force it to satisfy what the government takes to be its ethical obligations to a foreign populace will raise the dreaded specter of moral paternalism.

On a practical level, few of these issues present significant problems in the present context. By and large, most of the main players acknowledge that they need to weigh the effects of their actions on the Chinese people and that government intervention is necessary and desirable.[255] The problem is deciding how the theoretical model we have been developing could be utilized in situations involving less cooperative parties. Perhaps the ultimate lesson to be derived from all this is that a new theory of the state is required to take into account the moral and political realities created by the advent of the age of the transnational corporation. Just as the stakeholder may be replacing the stockholder as the focal point corporate life, it may be about time that the human being replaces the citizen in the life of nations.

---

[254] It would also provide theoretical justification for the government to exert pressure on the international community to become involved, as otherwise U.S. IT companies would stand to be harmed by increased competition from their unregulated European and Asian competitors.

[255] *See* Hearing, *supra* note 86, at 59, 61, 76.

V. CONCLUSION

We have argued in defense of a hybrid approach to regulating the activities of U.S. IT companies in China. What remains to be done is the much more difficult task of deciding how best to implement it. We have defended a policy of engagement. The lingering question is how far we should be willing to go in pursuit of it.

It is important to keep in mind here that the kinds of things that U.S. IT companies have been criticized for doing in China are sufficiently distinct as to warrant close individual attention. It is possible to distinguish at least four potential problem areas: (1) censoring results on search engines, (2) censoring content on blogs and websites, (3) tracking user activities and supplying their identities to the authorities, and (4) providing equipment and training that would facilitate one or more of the preceding activities, whether intentionally or through dual use application. There seem to be morally significant differences between them that should be taken into account when deciding how best to regulate the industry.

For example, we argued above that U.S. companies should not necessarily be prohibited from censoring politically sensitive search results. This is due in part to the fact that Chinese versions of U.S. search engines actually provide greater access to content than their domestic competitors. Even if this were not the case, however, censorship of this type simply deprives users of help in locating content on the web. It does not remove the content, and even moderately savvy users will be capable of finding it on their own, whether through the use of proxy servers or by some other means.

More problematic are cases in which U.S. IT companies are forced to comply with Chinese demands to censor content not otherwise available on the Internet. In these cases, the companies are not only hindering the free flow of information, but actively interfering with their users' speech. Moreover, there is no indication that U.S.-based content hosting services are less likely to censor their users' blogs or websites than Chinese companies are. It is possible,

however, to require them to make any content they are forced to censor within China available to users outside China. This would at least provide Chinese users with a broader forum for speech than they would otherwise be likely to have. It would also enable users within China to access the content through the use of proxy servers.

There should be absolutely no tolerance, however, for corporations that actively assist the authorities in tracking and monitoring their users. The Global Online Freedom Act acknowledges this interest by seeking to prevent companies from storing sensitive user information within China and imposing civil and criminal liability for companies that turn over such information except to comply with legitimate law enforcement purposes. The problem with this solution, of course, is that its efficacy would be subject to erosion by Chinese countermeasures. China might, for example, impose similar or even harsher penalties on companies that fail to collect and make this information available to the authorities. As we saw above, it already does something like this in its Internet cafe industry.[256] In such an event, it may ultimately become necessary to follow Google's present example and prevent U.S. IT companies from providing any services in China that require collecting this kind of information to begin with.

Perhaps the hardest question of all is what to do about companies like Cisco that provide the Chinese with equipment whose legitimate security features can be used to facilitate censorship and surveillance on a scale not matched by their competitors' products. Compounding the problem here is that these companies will inevitably be expected to provide technical support for the equipment as well. We could impose regulations preventing such companies from providing made-to-order equipment designed specifically for the purposes of censoring politically sensitive content. We could also attempt to prevent companies from providing detailed information on how to use the equipment for such purposes. But in the final analysis, neither of these two

[256] *See supra* Part II(C)(3).

solutions adequately addresses the fact that U.S.-made equipment is being used to create one of the most technologically sophisticated police states in the world today. It is arguable, certainly, that corporations should not be penalized for the uses to which their customers put their otherwise legitimate products. We also have an interest in ensuring that China does not begin purchasing proprietary hardware that would further isolate it from the rest of the world. Whether these are sufficient reasons to permit U.S. manufacturers of Internet-related hardware to continue doing business with China is a matter that will need to be addressed in the continuing public debate to which this Note is but a small and, admittedly, incomplete addition.