HONORS CAPSTONE: FALL 2010

Profit or Purpose

Legal and Ethical Issues for U.S. IT Companies in China

Caleb Skeath

12/11/2010

Advisor: Professor Michael Mass

General University Honors

Table of Contents

Introduction

The involvement of U.S. information technology companies in China dates back to 1978, when IBM sold its first mainframe computer to China.[1] The first major incursion into the Chinese market followed two decades later, when Yahoo! launched a Chinese language version of its search engine.[2] Other U.S. IT firms, including Microsoft, Google, and Cisco, have followed in Yahoo!'s footsteps by competing against domestic Chinese firms for a share of the massive Chinese IT market. Current estimates put the number of Chinese internet users at more than 200 million, a figure larger than any other country except the United States. Chinese Internet users also spend more time online than U.S. Internet users.[3]

However, the involvement of U.S. companies in the Chinese IT market is not without its dangers. Due to China's notorious Internet censorship regime, access to foreign websites can sometimes be slow, spotty, or nonexistent. As a result, many U.S. IT companies have set up subsidiaries in China and cooperated (to varying extents) with the Chinese government's censorship efforts in an effort to gain increased market share within China. The first rumbles of public discontent in the U.S. over American cooperation in Chinese Internet censorship began to surface earlier this decade, as human rights groups voiced their outrage over Yahoo!'s complicity in the arrest of several Chinese dissidents. After several of the arrested dissidents sued Yahoo! under the Alien Tort Claims Act (ATCA), Congress was "appalled" at what it saw as violations of basic human rights by U.S. companies in China.[4] Members of the House Committee on

---

[1] John H. Maier, "Information Technology in China," 20 *Asian Survey* 860, 872 (1980). Quoted in "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch*. Human Rights Watch, 9 Aug 2006. Web. 10 Oct 2010.

[2] Marc D. Nawyn, *Code Red: Responding to the Moral Hazards Facing U.S. Information Technology Companies in China,* 2007 Colum. Bus. L. Rev. 505 (2007)

[3] John Ng, "China's Economy Still Sizzling," *Asia Times Online*, Jan. 26, 2007, http://www.atimes.com/atimes/China Business/IA26Cb03.html. (retrieved November 7, 2010)

[4] Christopher Stevenson, *Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World,* 30 B.C. Int'l & Comp. L. Rev. 531 (2007)

International Relations held a joint hearing in February 2006 with the Subcommittee on Africa, Global Human Rights, and International Operations and the Subcommittee on Asia and the Pacific. At the hearing, entitled "The Internet in China: A Tool for Freedom or Suppression?," House representatives questioned executives of Yahoo!, Google, Microsoft, and Cisco Systems about their involvement in Chinese censorship, with some members of Congress asking the executives how they could sleep at night[5] The U.S. Department of State simultaneously announced the creation of the Global Internet Freedom Task Force to address the issue.[6]

In the years since, the issue of corporate complicity in Chinese Internet censorship has resurfaced repeatedly. After an NGO published a detailed account of Yahoo! handing over a political dissident's identifying information to Chinese authorities—which contradicted Yahoo! General Counsel Michael Callahan's 2006 testimony before Congress that Yahoo! "was not aware of the nature of the request [from Chinese authorities]"—Congress again summoned Yahoo! executives to testify at a hearing entitled "Yahoo! Inc.'s Provision of False Information To Congress.[7]" In May 2008, executives from the same four companies from the 2006 hearing were called before the Senate Subcommittee on Human Rights and the Law and urged to develop a code of conduct to guide their actions overseas.[8]

With the announcement by Google earlier this year of their decision to shut down their Chinese search engine following a cyberattack that originated in China, many U.S. IT companies

---

[5] The Subcommittees on Africa, Global Human Rights and International Operations, and Asia and the Pacific," U.S. House of Representatives Committee on International Relations, Joint Hearing: "The Internet in China: A Tool for Freedom or Suppression?" February 15, 2006, http://wwwc.house.gov/international_relations/109/cal021506.pdf (retrieved November 3, 2010)

[6] Mara D. Bryne, *When in Rome: Aiding and Abetting in Wang Xiaoning v. Yahoo*, 34 Brooklyn J. Int'l L. 151 (2008)

[7] "Yahoo! Inc.'s Provision of False Information to Congress," Hearing Before H. Comm. On Foreign Affairs, 110th Cong. (2007).

[8] Global Internet Freedom: Corporate Responsibility and the Rule of Law, Hearing Before S. Subcomm. on Human Rights and the Law, 110th Cong. (2008) (Opening Statement of Chairman Senator Dick Durbin).

are reconsidering their decision to conduct business in China.[9] This paper will examine the most relevant of those companies, as well as the legal constraints on their actions in China. The paper will seek to answer two main questions. First, what are the legal and ethical difficulties confronted by U.S. IT companies that do business in China? Second, what are the legal remedies available to ensure that these companies act in an ethical and legal manner, and are they effective?

In Part I of this paper, the structure of the Chinese Internet censorship system will be outlined, as well as the role of private companies within it. Part II will cover four separate case studies of U.S. IT companies operating within China—Yahoo!, Microsoft, Google, and Cisco Systems (the same four companies called before the House and Senate Committees). Finally, in Part III, this paper will examine various legal remedies available to control the actions of these companies in China, and evaluate their effectiveness.

Part I: Overview of Chinese Internet Censorship

China's system of internet censorship is famous throughout the world as one of the most sophisticated and opaque information control regimes. Unlike internet censorship in Saudi Arabia, where users are clearly notified for the reasons of censorship whenever they attempt to access a blocked page, Chinese users receive no notification of censorship when attempting to access banned material.[10] Even the list of keywords and topics filtered by the "Great Firewall of China," as China's internet censorship system is known in the media, has never been officially released to the public.

---

[9] David Drummond. "A new approach to China." *The Official Google Blog."* January 12, 2010. http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (retrieved October 30, 2010)

[10] OpenNet Initiative, "Internet Filtering in Saudi Arabia in 2004," http://www.opennetinitiative.net/studies/saudi/ (retrieved November 7, 2010).

Within the People's Republic of China, at least twelve different government bureaus have some authority over the Internet. The Ministry of Information Industry (MII) is technically in charge of the information technology industry and the tight controls placed upon it by the Chinese government. However, censorship policy, including decisions on what content is to be censored, is directed by the State Council Information Office and the Propaganda Department of the Chinese Communist Party. Input from other government and public security agencies is also taken into account, and the policy is then implemented by the MII.[11]

A Human Rights Watch estimate in 2001 placed the total number of official Internet regulations issued by the Chinese government at 60, not including the regulations also in place at the provincial and local level.[12] In recent years, regulations have been expanded to cover new technology (such as cell phones and smartphones), as well as new methods of communication and online content creation (such as blogging and video-sharing websites). Although it would be impossible to enforce all of the regulations at all times, the legal framework and its effect on Chinese Internet users and companies has effectively controlled the information available on the Internet in China.

Content Censorship Via Hardware

Once policy is decided, it is then implemented within the hierarchy of the Chinese internet infrastructure. China has nine state-licensed Internet Access Providers (IAPs), which are the source of connections to both domestic and foreign internet sites. For access to foreign internet sites, each of the IAPs relies upon one or more foreign Internet "backbones.[13]" Each of

---

[11] Eric Harwit and Duncan Clark. "Shaping the Internet in China: Evolution of Political Control Over Network Infrastructure and Content." *Asian Survey*, 41:3, May-June 2001, pp. 337-408. Quoted in "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch*. Human Rights Watch, August 9, 2006. (retrieved October 10, 2010).

[12] Human Rights Watch, "Freedom of Expression and the Internet in China," A Human Rights Watch Backgrounder, undated, http://www.hrw.org/backgrounder/asia/china-bck-0701.htm (retrieved November 8, 2010).

[13] OpenNet Initiative, "Internet Filtering in China 2004-2005: A Country Study," April 14, 2005

the Chinese IAPs sells internet access on a wholesale basis to a portion of the several thousand Chinese Internet Service Providers (ISPs). The ISPs then sell Internet access at retail prices to individual Chinese Internet users. Since the foreign "backbones" are the only way for Chinese Internet users to access foreign websites, China has effectively created a gigantic intranet that greatly limits the ability of its citizens to connect to the outside world.[14]

The hardware backbone of China's internet censorship regime is found in routers, physical devices that direct the movement of individual "packets" of data between networks. These devices, and their ability to enable information exchange between two Internet users, are essential to any Internet infrastructure. The vast majority of modern routers—including virtually all of those used as part of the Chinese Internet infrastructure—enable a network administrator to filter the data passing through the router by programming the router to block data meeting specific criteria from passing into or out of a network. Although filtering technology was originally intended to allow ISPs to defend their networks from viruses, worms, and spam, it can also be used to block political, religious, or other categories of data from entering or exiting the network.[15]

This second use of routers is a crucial element of the Chinese Internet filtering regime. Routers are used in three crucial junctures within the Chinese Internet infrastructure: between foreign websites and IAPs, between IAPs and ISPs, and between ISPs and individual web users. According to the Open Net Initiative's 2005 technical analysis of the Chinese Internet filtering regime, network administrators at Chinese IAPs have programmed thousands of Internet web site

---

http://www.opennetinitiative.net/studies/china/ (retrieved November 4, 2010); China Internet Network Information Center, "17th Statistical Survey Report on The Internet Development in China," January 2006 http://www.cnnic.net.cn/download/2006/17threport-en.pdf (retrieved November 3, 2010).

[14] Christopher Stevenson, *Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World,* 30 B.C. Int'l & Comp. L. Rev. 531 (2007)

[15] Steven Cherry. "The Net Effect." *IEEE Spectrum,* June 2005. http://www.spectrum.ieee.org/print/1219 (retrieved November 3, 2010).

addresses (or URLs) and keywords into the Internet routers that provide connections between Chinese Internet ISPs and the IAPs, as well as the routers that provide connections between the IAPs and foreign websites. These "forbidden" addresses and keywords are also programmed into the routers at the ISP level, affecting the exchange of information between the ISP and individual internet users.[16]

Content Censorship Via Software

In addition to the censorship capabilities provided by Internet routers, the Chinese government has also developed its own filtering software to provide an additional layer of protection. Similar filtering programs are often used on a smaller scale by households, companies, and other organizations in order to restrict the websites that can be accessed by employees, students, or other users. Many other countries that engage in Internet censorship also use similar software, but most use a software program called SmartFilter from Secure Computing.[17] In China, the homegrown filtering software is deployed at the IAP and ISP level, in order to conduct additional filtering of political content. The majority of this filtering is focused on external websites that are accessed via the Internet "backbones" used by the IAPs. When a user enters the URL for a website that is blocked by filtering software, they receive a standard error message in their browser, which does not mention that the site has been filtered. An identical error message can result from any one of a number of different issues, including a failure in the Internet connection or user error. As a result, most users in China likely have no idea that their Internet browsing experience is being censored. In contrast, Saudi Arabia directs users to a page informing the user that they have attempted to access content that has been

[16] OpenNet Initiative, "Internet Filtering in China 2004-2005: A Country Study," April 14, 2005 http://www.opennetinitiative.net/studies/china/ (retrieved November 4, 2010)
[17] Ibid. See also Nart Villeneuve. "The Filtering Matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace." *First Monday*, Vol. 11, Number 1, January 2006, http://www.firstmonday.org/issues/issue11_1/villeneuve/index.html (retrieved November 5, 2010)

blocked in accordance with national law. The Saudi Arabian page includes contact information for a user to report a site that they believe has been blocked in error—an option that does not exist in the Chinese system.[18] China has frequently been criticized for the lack of transparency in their Internet filtering, as installing a customizable page to advise users that content has been blocked is relatively easy to do with modern filtering software.[19]

Content Censorship at the ISP/ICP Level

In addition to filtering technology, the Chinese Internet censorship regime also relies heavily on controls placed upon Internet Service Providers (ISPs) and Internet Content Providers (ICPs). In China, ISPs are often privately-held business, sometimes with foreign investment. ICPs are the individuals or organizations who provide publicly available content on the Internet, or who provide platforms on which users can communicate or create their own content. ICPs can range from news websites to chat rooms to video-sharing or blogging sites.

In China, ISPs are held liable for hosting politically objectionable content on any website accessed through their servers.[20] In a similar manner, ICPs are required to register for and display a license in order to operate legally in China, and are held liable for all content that appears on their website, regardless of whether the content was generated by employees of the ICP or by a site user or visitor. A condition of both obtaining and keeping a license to operate is that an ICP will prevent the appearance of politically objectionable content on its websites, either

[18] OpenNet Initiative, "Internet Filtering in Saudi Arabia in 2004," http://www.opennetinitiative.net/studies/saudi/ (retrieved November 7, 2010).
[19] Derek E. Bambauer, *Cybersieves*, 59 Duke L.J. 377 (2009)
[20] Eric Harwit and Duncan Clark. "Shaping the Internet in China: Evolution of Political Control Over Network Infrastructure and Content." *Asian Survey*, 41:3, May-June 2001, pp. 337-408. Quoted in "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch*. August 9, 2006. (retrieved October 10, 2010).

through automated means (filtering software) or by manually inspecting content created by users and removing any objectionable material.[21]

This obligation on the part of ICPs is outlined in the "Public Pledge on Self-Discipline for the Chinese Internet Industry," a document authored by the Internet Society of China (ISOC). Although the ISOC, the main professional organization for the internet industry in China, claims to be a nongovernmental organization (NGO), it is overseen by the Ministry of Information Industry (MII), which is in charge of implementation of Chinese Internet censorship policy. The "voluntary" pledge urges signatories to engage in "energetic efforts to carry forward the rich cultural tradition of the Chinese nation and the ethical norms of the socialist cultural civilization" by adhering to the industry regulations set up by the MII. The pledge also calls for companies, organizations, and individuals to refrain "from producing, posting, or disseminating pernicious information that may jeopardize state security and disrupt social stability.[22]" Within a year of the Pledge's introduction, more than 300 companies had agreed to abide by its terms.[23]

The presence of any content on a website that could be deemed "politically objectionable" may result in warnings from the MII, the State Council Information Office, the Communist Party's Propaganda Department, or various state security agencies. These warnings, directed at the management or employees of the ICPs, often threaten companies with revocation of their state-granted licenses if more stringent content controls are not implemented. In order to maintain their license, ICPs must ensure that prohibited content is not displayed on their websites.

---

[21] OpenNet Initiative, "Analysis of China's Non-Commercial Web Site Registration Regulation," February 22, 2006, http://www.opennetinitiative.net/bulletins/011 (retrieved November 3, 2010)
[22] Internet Society of China, "Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry" July 19, 2002, http://www.isc.org.cn/20020417/ca102762.htm (retrieved November 4, 2010).
[23] Jill R. Newbold, *Aiding the Enemy: Imposing Liability on U.S. Corporations For Selling China Internet Tools to Restrict Human Rights,* 2003 U. Ill. J.L. Tech. & Pol'y 503 (2003).

One of the interesting contradictions of Chinese Internet censorship is that the Chinese government does not provide ICPs with lists of prohibited words or phrases, nor does it mandate certain methods of censorship. Instead, all ICPs independently develop and maintain their own extensive lists of sensitive words or phrases. These lists are generated based on a combination of educated guesswork and trial-and-error. Companies include terms that are widely known to be politically sensitive in addition to terms that are referenced by Chinese officials, either in official meetings or in complaints that the companies receive from the Chinese government.

For content sharing services (such as video sharing and blogging websites), these words or phrases can either be automatically blocked or can be "flagged" for later inspection and possible manual removal by employees. In a similar manner, search engines maintain lists of thousands of words, phrases, and web addresses that will be filtered out of search results to prevent users from viewing links for or accessing prohibited websites. Although most of these websites are already blocked at the ISP level, their exclusion from search results provided by ICPs prevents Chinese internet users from knowing that these websites exist at all.[24] In two separate cases, a list of blocked terms from a Chinese company has leaked to U.S. sources, providing insights into the terms contained on such lists.[25]

As part of the process of generating lists of blocked content, some ICPs operating in China will even run diagnostic tests to determine which words, phrases, and web addresses are currently being blocked by the Chinese authorities at the router level. ICPs will then add any

---

[24] Rebecca MacKinnon, "Flatter World and Thicker Walls? Blogs, Censorship and Civic Discourse in China" in Daniel Drezner and Henry Farrell, eds., *The Political Promise of Blogging* (Ann Arbor: University of Michigan Press, publication pending), draft version under the title "Chinese Blogs: Censorship and Civic Discourse" at http://rconversation.blogs.com/rconversation/files/mackinnon_chinese_blogs_chapter.pdf (retrieved November 6, 2010).

[25] Xiao Qiang, "The words you never see in Chinese cyberspace," *China Digital Times*, August 30, 2004, http://chinadigitaltimes.net/2004/08/the_words_you_n.php (retrieved November 4, 2010). See also "Keywords Used to Filter Web Content," in series "The Great Firewall of China," *Washington Post*, February 18, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/02/18/AR2006021800554.html (retrieved November 4, 2010).

additional items to their lists, without being first asked to do so by the government. According to a 2006 report by the Human Rights Watch, many managers of Chinese ICPs are overcautious in their censoring efforts in an attempt to avoid getting into trouble with Chinese authorities. By using the fear of licensing issues, the Chinese government has managed to "outsource" a large portion of the work of censoring the Internet in China to the thousands of Chinese ICPs.[26] This agreement between the Chinese government and Western ICPs—in which the government exchanges permission to operate within China for the cooperation of the Western ICP in censorship efforts—has been criticized as ethically "appalling" by Western legal scholars.[27]

Censorship of Internet Communications (Email and Chat/Instant Messanging)

In the vast majority of the world, including China, email services hosted on servers located inside a country's borders are expected to comply with legitimate requests from law enforcement for information contained on those servers. This information includes, but is not necessarily limited to, user information and copies of email communications. However, the range of circumstances under which Chinese law enforcement bodies can make legitimate requests for user information and communications include elements of political speech that have been protected by international law. Due to the potential liability and public relations ramifications of being subjected to such requests by Chinese law enforcement, almost all Western IT companies in China do not offer email services. Yahoo!, as the one exception, offers email services with user data hosted on servers located within China. In addition, mobile and Internet chat services are subject to the same licensing requirements within China as all other ICPs, and are required to filter content deemed to be "politically sensitive" either by the Chinese

[26] Anne S.Y. Cheung, *The Business of Governance: China's Legislation on Content Regulation in Cyberspace,* 38 N.Y.U. J. Int'l L. & Pol. 1 (2005).
[27] Jill R. Newbold, *Aiding the Enemy: Imposing Liability on U.S. Corporations For Selling China Internet Tools to Restrict Human Rights,* 2003 U. Ill. J.L. Tech. & Pol'y 503 (2003).

government or by the chat service itself. One of the largest Western providers of chat services, Skype, admitted to including censorship functions in the Chinese-language version of its software, which was developed in cooperation with Tom Online, a Chinese company.

Methods of Circumventing Censorship Efforts

Despite the Chinese government's best efforts, some holes in the "Great Chinese Firewall" do exist. The most widely-used circumvention effort is the use of a proxy server, which is an intermediary server designed to hide the end user's true location. If a Chinese user utilizes a proxy server to access websites that are normally blocked by Chinese Internet filtering, the filtering software and router filters will only see that the Chinese user is accessing the proxy server, instead of seeing all of the sites the user is accessing through the proxy server. The Internet will be noticeably slower for the Chinese user, however, since the information must travel through the proxy server in addition to any other servers it normally encounters.

Although lists of proxy servers can be found on the Internet, the Internet Protocol (IP) addresses of these servers are blocked by administrators on some level of the Chinese Internet infrastructure, usually within hours. Once a proxy server's IP address is blocked, it becomes impossible to use. As a result, Chinese users who use proxy servers must not only contend with a slower internet experience, but also switch to a new proxy server every thirty minutes to two hours. A number of software tools have been developed to help users utilize proxy servers, either by providing updates of new proxy servers or by configuring the software to automatically search for and connect to new, unblocked proxy servers.[28]

A survey by the Chinese Academy of Social Sciences (CASS) in 2000 found that only 10 percent of Chinese Internet users regularly used proxy servers to surf the Web. Although 25%

[28] Tom Spring, "Outsmarting the Online Privacy Snoops," *PC World*, February 28, 2006, http://www.pcworld.com/news/article/0,aid,124891,00.asp (retrieved November 7, 2010).

reported "occasional" usage of proxy servers, only 0.6% identified themselves as "frequent" users of proxy servers.[29] Although these numbers may be affected by Chinese internet users' reluctance to admit to using proxy servers, there is no denying that the difficulty of locating a proxy server, in addition to the subpar Internet service provided by them, has discouraged many Chinese Internet users from seeking out unfiltered Internet sources. However, a 2005 CASS survey indicated that Chinese Internet censorship efforts did not have the full support of the population. Although the majority of Internet users surveyed agreed that the government should control violent and pornographic content on the Internet, only 12 percent felt that controlling political content was a good idea.[30]

Part II: Case Studies: Yahoo! Inc.

In 1999, Yahoo! became the first major U.S. internet content company to enter the Chinese market by opening a Beijing office and unveiling a Chinese-language search engine.[31] Three years later, Yahoo! signed the "Public Pledge on Self-discipline for the Chinese Internet Industry," becoming the first (and only) Western company to sign the pledge. The move met with significant protest from Western human rights groups, who claimed that Yahoo! was engaging in voluntary censorship and collusion with the Chinese government by signing the non-voluntary pledge. One legal scholar accused Yahoo! of "[taking] the lead in bowing under pressure" from the Chinese government to cooperate in censorship efforts.[32] Yahoo! defended

---

[29] Guo Liang and Bu Wei, "Survey report of Internet use and its influence: Beijing, Shanghai, Guangzhou, Chengdu and Changsha 2000." (Beijing: Chinese Academy of Social Sciences, 2001). Quoted in "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch*. August 9, 2006. (retrieved October 10, 2010).

[30] Chinese Academy of Social Sciences, "Surveying Internet Usage and Impact in Five Chinese Cities." Quoted in "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch*. August 9, 2006. (retrieved October 10, 2010).

[31] "Yahoo! Introduces Yahoo! China," Yahoo! corporate press release, September 24, 1999, http://docs.yahoo.com/docs/pr/release389.html (retrieved November 7, 2010).

[32] Surya Deva, *Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?*, 39 Geo. Wash. Int'l L. Rev. 255 (2007)

its actions by claiming that "the restrictions on content contained in the pledge impose no greater obligation than already exists in laws in China.[33]" Although Yahoo!'s claim was true at the time, neither Microsoft nor Google has become a signatory to the Public Pledge despite setting up operations as an ICP in China.

Yahoo!'s Chinese search engine (http://cn.yahoo.com) maintains a list of thousands of banned terms that are automatically filtered out of search results. In addition, Yahoo! has also de-listed websites, meaning that each de-listed website is skipped over when the search engine searches the Internet for results to a particular User entry. According to the Human Rights Watch, sites de-listed on Yahoo!'s Chinese search engine include Radio Free Asia and the *New York Times*. In other cases, searches on Yahoo! China will result in one of several error messages instead of the results of the search.

Yahoo! is also the only major Western ICP to offer email services in China, as it provides Chinese-language email at yahoo.com.cn. Yahoo! executives have previously confirmed that Yahoo!'s email servers for Chinese users are located in China, therefore subjecting them to disclosure requests from Chinese law enforcement.[34] As a result, Yahoo! has been implicated as providing data to Chinese law enforcement that assisted in the prosecution and conviction of political dissidents in at least four separate cases.

In September 2003, Chinese political dissident Wang Xiaoning was sentenced to ten years in prison for "incitement to subvert state power." Xiaoning was an Internet writer who distributed various essays via email and Yahoo! Groups that led to his arrest and conviction.

---

[33] Jim Hu, "Yahoo yields to Chinese web laws," *CNet News*. Quoted in "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch*. Human Rights Watch, 9 Aug 2006. Web. 10 Oct 2010.

[34] "Testimony of Michael Callahan, Senior Vice President and General Counsel, Yahoo! Inc., Before the Subcommittees on Africa, Global Human Rights and International Operations, and Asia and the Pacific," U.S. House of Representatives Committee on International Relations, Joint Hearing: "The Internet in China: A Tool for Freedom or Suppression?" February 15, 2006, http://wwwc.house.gov/international_relations/109/cal021506.pdf, and Yahoo! corporate press release, undated, http://yhoo.client.shareholder.com/press/ReleaseDetail.cfm?ReleaseID=187725 (both retrieved November 6, 2010).

According to a court judgment obtained by the group Human Rights in China, Yahoo! provided information to Chinese investigators pertaining to the email address and Yahoo! group used by Xiaoning to distribute his material.[35] On the basis of this assistance, Xiaoning's wife later filed a claim on his behalf against Yahoo! in U.S. Federal Court. The suit, filed under the Alien Tort Claims Act, accused Yahoo! of aiding and abetting torture and human rights violations by the Chinese government. Although the suit was settled out of court in 2006, Yahoo! received highly negative publicity as a result of the Xiaoning lawsuit.

Although the Xiaoning case is the most notable of Yahoo!'s collaboration with Chinese law enforcement, it was not the only such incident. In November 2003, Jiang Lijun was sentenced to four years in prison for "subversion." According to court transcripts, Lijun, an Internet writer and pro-democracy activist, sent emails through an anonymous Yahoo! email account that contained politically sensitive information. These emails were later provided to Chinese authorities by Yahoo!.[36] In December 2003, Internet writer Li Zhi was sentenced to eight years in prison for "inciting subversion of state authority." In Zhi's case, Yahoo! provided user account information regarding Zhi to the Chinese government.[37] In April 2005, Chinese journalist Shi Tao was sentenced to ten years in prison for "divulging state secrets abroad." According to court documents, Yahoo! released information from a Yahoo! email account connected to Yahoo! China in response to Chinese government requests. The information

---

[35] The original document and translation are at http://hrichina.org/public/contents/press?revision%5fid=27803&item%5fid=27801 (retrieved November 9, 2010).
[36] The original Chinese court document and English translation are at http://www.rsf.org/article.php3?id_article=17180 (retrieved November 7, 2010).
[37] For a partial English translation see http://chinadigitaltimes.net/2006/02/yahoo_helped_sentence_another_cyber_dissident_to_8_year_1.php (retrieved November 7, 2010)

disclosed by Yahoo! linked Shi Tao to documents that had been posted on a U.S.-based dissident website.[38]

In response to criticism over their handling of the cases mentioned above, Yahoo! cited the location of its servers within China and under the control of Yahoo! China employees as evidence that it had no choice but to release the information. Michael Callahan, general counsel for Yahoo!, stated that "[w]hen we receive a demand from law enforcement authorized under the law of the country in which we operate, we must comply.[39]" Callahan further claimed that the Chinese government, in the same manner as many governments worldwide, provides no information about the nature of the case in their requests, making it impossible to determine if a case is politically motivated.[40] Learning from Yahoo!'s troubles, neither Microsoft nor Google have opted to store user data within China, and neither company has offered email services to Chinese consumers.

In August 2005, Yahoo! announced that it planned to purchase a 40% stake in Alibaba.com, a Chinese e-commerce company. As part of the deal, Yahoo! merged its Chinese search engine and Chinese email service with Alibaba. After the deal was complete, Yahoo! controlled one of the four seats on the Alibaba.com board of directors. However, Alibaba.com continued to operate Yahoo!'s Chinese businesses under the Yahoo! brand name. According to legal experts, the purpose of this move from Yahoo!'s perspective was to avoid responsibility for its actions in China, including cooperation with Internet censorship.[41] As Michael Callahan

---

[38] Reporters Sans Frontières, "Information supplied by Yahoo! helped journalist Shi Tao get 10 years in prison," September 6, 2005 http://www.rsf.org/article.php3?id_article=14884 (retrieved November 7, 2010).
[39] "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch*. August 9, 2006. (retrieved October 10, 2010).
[40] "Yahoo Writer Jailed in China." *Red Herring*. February 9, 2006, http://www.redherring.com/Article.aspx?a=15659&hed=Yahoo+Writer+Jailed+in+China (retrieved November 7, 2010).
[41] Surya Deva, *Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?*, 39 Geo. Wash. Int'l L. Rev. 255 (2007)

explained to a 2006 House of Representatives committee hearing, "Alibaba.com is the owner of the Yahoo! China businesses, and that as a strategic partner and investor, Yahoo!...does not have day-to-day operational control over the Yahoo! China division of Alibaba.com.[42]"

Yahoo! has defended its practices in China by claiming that providing censored information in China is better than having no information provided at all.[43] In the days before the Congressional hearings in 2006, Yahoo! released a document entitled "Our Beliefs as a Global Internet Company." The document detailed Yahoo!'s commitment to maintaining "the open availability of the Internet around the world," both by narrowly enforcing censorship restrictions and promoting "the principles of freedom of speech and expression.[44]" As part of their efforts at increased transparency, Yahoo! China began running a disclaimer notice at the end of pages of a censored search, stating in Chinese that "[a]ccording to relevant laws and regulations, some search results may not appear."

Yahoo!'s troubles did not end in 2006, however. After new reports emerged in 2008, revealing that Yahoo! had provided Chinese authorities with information leading to dissident arrests, Congress summoned Yahoo! executives once again for a hearing entitled "Yahoo!'s Provision of False Information to Congress." At the hearing, Yahoo! executives were grilled by Congressional representatives. U.S. Representative Tom Lantos (R-CA) called the executives moral "pygmies" for cooperating with the Chinese requests.[45]

---

[42] "Testimony of Michael Callahan, Senior Vice President and General Counsel, Yahoo! Inc., Before the Subcommittees on Africa, Global Human Rights and International Operations, and Asia and the Pacific," U.S. House of Representatives Committee on International Relations, Joint Hearing: "The Internet in China: A Tool for Freedom or Suppression?" February 15, 2006, http://wwwc.house.gov/international_relations/109/cal021506.pdf (retrieved November 7, 2010).

[43] Nate Anderson, "Yahoo on China: We're doing some good," *Ars Technica*, May 12, 2006, http://arstechnica.com/news.ars/post/20060512-6823.html (retrieved November 6, 2007).

[44] "Yahoo!: Our Beliefs as a Global Internet Company," Yahoo! corporate press release, undated, http://yhoo.client.shareholder.com/press/ReleaseDetail.cfm?ReleaseID=187401 (retrieved November 6, 2010).

[45] Bruce Einhorn. "In China, Google Fallout Damages Yahoo!" *BusinessWeek.* January 19, 2010. http://www.businessweek.com/globalbiz/content/jan2010/gb20100119_789082.htm (retrieved November 4, 2010).

In 2008, Chinese dissidents Guo Quan and Zheng Cunzhu filed suit against Yahoo! under both the Alien Tort Claims Act and the Torture Victims Protection Act. Quan claimed that as a result of censorship of his name on Yahoo!'s Chinese search engine, he lost business at his garment company. Cunzhu was living in the U.S. and claimed he was not able to return to China as a result of Yahoo!'s handover of emails and user data to the Chinese authorities, which had implicated Cunzhu as a political dissident.[46] The lawsuit alleged "violation of international law including torture and prolonged detention, as well as unfair business practices, intentional infliction of emotional distress, false imprisonment and assault.[47]"

At the same time the lawsuit was filed, Yahoo! CEO Jerry Yang responded to pressure from human rights activists by sending a letter to then-Secretary of State Condolezza Rice, asking for the U.S. government's help in persuading China to release imprisoned political dissidents. Yang specifically cited the cases of Shi Tao and Wang Xiaoning, the prisoners who had sued Yahoo! for its role in their detention.[48] As of the writing of this paper, both Xiaoning and Tao are still imprisoned in China.

Yahoo! has changed its stance on business in China over the past few years in response to heavy public criticism. Following Google's announcement that it was considering pulling out of China over censorship concerns, Yahoo! stated that it was "aligned" with Google's stance.[49] Alibaba.com chairman Jack Mao, who is in charge of Yahoo! China operations, called Yahoo!'s statement "reckless" and claimed that he had "no idea" who was responsible for the cyberattacks

---

[46] Nate Anderson. "Who needs lawyers? Two more Chinese dissidents sue Yahoo." *Ars Technica*. February 29, 2008. http://arstechnica.com/tech-policy/news/2008/02/who-needs-lawyers-two-chinese-dissidents-sue-yahoo.ars (retrieved November 8, 2010)
[47] Elinor Mills. "Yahoo Sued by Chinese Dissidents Again." *CNet News.* February 27, 2008. http://news.cnet.com/8301-10784_3-9881042-7.html (retrieved November 8, 2010)
[48] Ibid.
[49] Bruce Einhorn. "In China, Google Fallout Damages Yahoo!" *BusinessWeek*. January 19, 2010. http://www.businessweek.com/globalbiz/content/jan2010/gb20100119_789082.htm (retrieved November 2, 2010)

on Google that prompted Google to consider withdrawing from the Chinese market.[50] Following this public dispute between Yahoo! and Alibaba.com, which controls Yahoo! China, Alibaba.com began redirecting resources away from the development of Yahoo! China. Yahoo! China currently holds only 3% market share in China.[51]

Part II: Case Studies: Microsoft, Inc.

Microsoft has been involved in China since 1992, mainly through sales of hardware and software as well as research and development efforts. Microsoft did not shift into the role of an ICP until 2005, when it formed a joint venture between Microsoft Network (MSN) and Shanghai Alliance Investment Ltd. (SAIL) to create MSN China. MSN China unveiled a Chinese-language version of the MSN online portal in mid-2005.[52]

As part of its services, MSN China offers users the ability to create their own blogs and publish their own content on the blogs they have created. Within a month of the introduction of MSN China's online portal, users discovered that Microsoft was censoring words such as "democracy" and "freedom" from the titles of its blogs.[53] Further independent testing in December 2005 uncovered that Microsoft had extended censorship into the titles of individual blog posts. A blog posting containing a banned term would typically be removed, and the entire blog shut down, within the span of a few days.

Microsoft had to deal with its own censorship uproar at the end of 2005, when it shut down a blog belonging to Zhao Jing, a Chinese journalist and blogger. Jing, writing under the pseudonym Michael Anti, had started a blog on MSN Spaces in August 2005 after his previous

---

[50] Bruce Einhorn. "In China, Google Fallout Damages Yahoo!" *BusinessWeek*. January 19, 2010. http://www.businessweek.com/globalbiz/content/jan2010/gb20100119_789082.htm (retrieved November 2, 2010)

[51] Ibid.

[52] "Microsoft Prepares to Launch MSN China," Microsoft news release, May 11, 2005, http://www.microsoft.com/presspass/press/2005/may05/05-11MSNChinaLaunchPR.mspx (retrieved November 3, 2010).

[53] "Screenshots of Censorship," *Global Voices,* June 16, 2005, http://www.globalvoicesonline.org/?p=238; and http://news.bbc.co.uk/1/hi/technology/4088702.stm (retrieved November 5, 2010).

blog on another blogging website had been shut down by Chinese authorities.[54] After propaganda authorities cracked down on the *Beijing News*, firing the editors and deputy editors, Jing's blog covered the crackdown and subsequent protests and walkouts by the staff of *Beijing News*. Jing voiced his support for the protests on his blog, and called for a reader boycott of the newspaper under its new leadership. On December 30, 2005, his blog was shut down. Microsoft later told the *New York Times* that Jing's blog had been deleted by the MSN Spaces staff "after Chinese authorities made a request through a Shanghai-based affiliate of the company.[55]"

As a result of the public's reaction to the deletion of blogs on MSN Spaces, Microsoft announced a change to its blog censorship policy in China.[56] It announced the changes during testimony by its representatives before the House of Representatives in January 2006.[57] Microsoft pledged to only remove content when it received a legally binding request from the government in which Microsoft or its affiliates were based, and only when the content either violated local law or MSN's terms of use. In addition, Microsoft promised that content would only be removed in the country requesting the removal of the content. Owing to new capabilities in the MSN Spaces programming infrastructure, Microsoft would be able to block access to the content in the area where it was requested to be blocked while maintaining access to the blocked content for users in all other regions. Finally, Microsoft promised increased transparency by

---

[54] Roland Soong, "The Anti Blog is Gone," *EastSouthWestNorth,* December 31, 2005, http://www.zonaeuropa.com/200512brief.htm#100 (retrieved November 7, 2010); and Rebecca MacKinnon, "Microsoft Takes Down Chinese Blogger," *RConversation.com,* January 3, 2006, http://rconversation.blogs.com/rconversation/2006/01/microsoft_takes.html (retrieved November 7, 2010).

[55] David Barboza and Tom Zeller, Jr., "Microsoft Shuts Blog's Site After Complaints by Beijing," *New York Times*, January 6, 2006, http://www.nytimes.com/2006/01/06/technology/06blog.html?ex=1294203600&en=f785b99efa4cf025&ei=509&partner=rssuserland&emc=rss (retrieved November 7, 2010).

[56] Nellie L. Viner, *The Global Online Freedom Act: Can U.S. Internet Companies Scale the Great Chinese Firewall at the Gates of the Chinese Century?,* 93 Iowa L. Rev. 361 (2007)

[57] Jeremy Kirk, "Microsoft revamps blogging policy," *InfoWorld*, January 31, 2006, http://www.infoworld.com/article/06/01/31/74926_HNmicrosoftbloggingpolicy_1.html (retrieved November 6, 2010).

notifying users when content has been blocked due to government restrictions, and the reason for the blockage.[58]

As a result of Microsoft's revised policy, a number of politically sensitive blogs have remained visible in China, including several kept by family members of imprisoned political dissidents who blog about their efforts to free their loved ones. Some blogs are still removed, although it is impossible to tell whether this removal is in response to official Chinese government requests or whether removal is initiated by MSN Spaces staff. As of the end of 2005, MSN Spaces had become the most popular blogging site in China, hosting more blogs than any other Chinese language blog-hosting service.[59]

Following the highly successful launch of MSN Spaces in China, Microsoft launched a test version of its Chinese search engine in January 2006. The search engine was integrated into the MSN China portal soon after its launch.[60] Independent testing of the search engine by editors at C-Net News showed that while the MSN search engine linked to a number of sites that were blocked by both Yahoo! and Google search (such as the Human Rights Watch), it also blocked other sites that were accessible through Google and Yahoo! (such as Time.com).[61] MSN also de-listed some websites from the Chinese version of its search engine, according to the Human

---

[58] Testimony of Jack Krumholtz, Associate General Counsel and Managing Director, Federal Government Affairs, Microsoft Corporation to the House of Representatives Committee on International Relations Joint Hearing of the Subcommittee on Africa, Global Human Rights and International Operations and the Subcommittee on Asia and the Pacific: "The Internet in China: A Tool for Freedom or Suppression?" February 15, 2006, http://wwwc.house.gov/international_relations/109/kru021506.pdf (retrieved November 3, 2010).

[59] "MSN Spaces rated the leading blog service provider in China," *People's Daily Online*, December 20, 2005, http://english.people.com.cn/200512/20/eng20051220_229546.html (retrieved November 7, 2010).

[60] Eric Wan, "MSN Launches Chinese Search Beta," *Pacific Epoch*, January 6, 2006, http://www.pacificepoch.com/newsstories/50283_0_5_0_M/ (retrieved November 7, 2010); and "Beta Version of Chinese MSN Search Available," *China Net Investor* reproducing *Shanghai Times*, January 15, 2006, http://china-netinvestor.blogspot.com/2006/01/beta-version-of-chinese-msn-search.html (retrieved November 7, 2010).

[61] Declan McCullagh, "No booze or jokes for Googlers in China," *CNET News*, January 26, 2006, http://news.com.com/What+Google+censors+in+China/2100-1030_3-6031727.html?tag=nefd.lede (retrieved November 5, 2010).

Rights Watch.[62] The MSN Chinese search engine frequently included a warning on censored searches at the bottom of the page that read: "The search results have omitted some content. Click here to find out why." The hyperlink in the warning took users to a FAQ page about MSN's Chinese portal. Under the heading "When there are no search results or filtered search results," the page advised that "according to local unwritten rules, laws, and regulations, inappropriate content cannot be displayed." The page then recommended for users to alter the wording of the original search.[63]

According to the legal experts, Microsoft has taken note of Yahoo!'s difficulties in providing email services to Chinese users.[64] Since Yahoo! has chosen to locate the user data for its Chinese email service on servers inside China, employees of Yahoo! China have been subjected to, and forced to comply with, requests from Chinese law enforcement for user data from Yahoo! Chinese-language email accounts. Wishing to avoid these difficulties, Microsoft has not yet provided its Hotmail service in a Chinese-language format with user data stored on servers within China. Microsoft has had previous success in refusing Chinese government requests for Hotmail user data, arguing that the data is not located in China and therefore is not under Chinese jurisdiction.[65]

In response to Google's decision to pull out of China in March 2010, Microsoft announced its intention to continue its presence in China. They stated an intention to continue to obey local laws and censorship requirements. A spokesman defended Microsoft's decision to continue censorship, adding that "engagement in global markets is important…all technology

---

[62] "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch*. August 9, 2006. (retrieved October 10, 2010).
[63] The explanatory page is located on MSN's Chinese search website at http://beta.search.msn.com.cn/docs/help.aspx?t=SEARCH_CONC_AboutSearchResults.htm&FORM=HRRE#4 (retrieved November 7, 2010)
[64] Surya Deva, *Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?*, 39 Geo. Wash. Int'l L. Rev. 255 (2007)
[65] Ibid

companies should make public commitments to help protect Internet users." As part of their commitment, Microsoft has held firm on its decision to not offer Hotmail to Chinese customers, due to potential requirements to hand over user data to Chinese authorities.[66]

Part II: Case Studies: Google, Inc.

Google's experiences in China have drawn perhaps the most attention out of any multinational corporation, both because of its reputation for user transparency and its motto, "Don't be evil." In September 2000, the company unveiled its Chinese-language search engine. Google's first run-in with Chinese authorities occurred two years later, when Google.com was temporarily blocked on Chinese ISPs by the Chinese government. Users who attempted to access Google.com were instead redirected to other Chinese search engines. Google stated that they were working with the Chinese authorities to restore access, which occurred after two weeks.[67] Google co-founder Sergey Brin insisted that Google had not negotiated with the Chinese government to lift the block. Instead, Brin claimed that "popular demand" for Google.com had forced Chinese authorities to restore access.

Despite Google's claim of victory over the Chinese Internet censorship regime, independent testing in 2004 revealed that "not all of [Google's] functions are available" to users within China.[68] As Google had not yet established a physical location within China, the Chinese government could not force Google to filter its search results by threatening to revoke its business license. Instead, Google was censored by the employees of the Chinese government and Chinese ISPs. China used filtering at the ISP router level to block access to Google's

---

[66] Tania Branigan. "We're staying in China, says Microsoft, as free speech row with Google grows." *The Guardian.* March 25, 2010. http://www.guardian.co.uk/technology/2010/mar/25/china-microsoft-free-speech-google (retrieved November 7, 2010)

[67] Jason Dean, "As Google Pushes into China, It Faces Clash With Censors," *Wall Street Journal*, December 16, 2005, http://online.wsj.com/article/SB113468633674723824.html (retrieved November 3, 2010).

[68] OpenNet Initiative, "Google Search & Cache Filtering Behind China's Great Firewall," Bulletin 006, August30, 2004, http://www.opennetinitiative.net/bulletins/006/ (retrieved November 3, 2010).

"cache" feature (which allows users to view an earlier snapshot of the webpage, even if the page has since been removed from the web). In addition, China blocked access to Google search results themselves. When users clicked on a link to a banned website that was included in Google's search results, they would receive an error page, without any explanation about the error or censorship. If a user attempted to search for a banned word or phrase, the user's connection to Google was terminated and no search results were received.[69]

Google launched a Chinese-language version of its Google News service in September 2004. For the first time, a Google product implemented some censorship elements in response to the Chinese censorship regime instead of allowing the Chinese government and ISP employees to censor it. When a user's news search yielded blocked results, those results were not displayed by Google News. In response to criticism over the move, Google posted an entry on its official blog addressing the topic. In the blog post, Google acknowledged that "there would be some small user value to just seeing" the links to the blocked news stories, but including these links in a results list "would likely result in Google News being blocked altogether in China.[70]"

In December 2005, Google took another step towards greater involvement in the Chinese market by receiving its license to operate as an ICP in China. On January 26, 2006, Google launched a Chinese-language version of its search engine, Google.cn, which censored thousands of keywords and web addresses.[71] According to experts, Google.com had been inaccessible to Chinese users up to 10% of the time prior to Google setting up a specific search engine for Chinese users and cooperating with Chinese censors. Entry into the Chinese market by Yahoo!

---

[69]OpenNet Initiative, "Google Search & Cache Filtering Behind China's Great Firewall," Bulletin 006, August30, 2004, http://www.opennetinitiative.net/bulletins/006/ (retrieved November 3, 2010).
[70] "China, Google News and source inclusion," *Google Blog,* September 27, 2004, http://googleblog.blogspot.com/2004/09/china-google-news-and-source-inclusion.html (retrieved November 6, 2010).
[71] OpenNet Initiative, "Google.cn Filtering: How It Works," January 25, 2006, http://www.opennetinitiative.net/blog/?p=87 (retrieved November 6, 2010).

and Microsoft had allowed these companies to set up search engine operations that were faster and more effective than Google.com.[72] By setting up a Chinese-language version of its search engine and complying with the Chinese censorship regime, Google acknowledged that self-censoring results for Chinese users through Google.cn produced a superior user experience than allowing Chinese authorities to censor the results available to Chinese users on Google.com.[73]

As with many other search engine companies, Google had created its own list of blocked terms and keywords based upon testing of what terms and web addresses were being blocked by Chinese ISPs.[74] Google also de-listed websites from its Google.cn search engine, but Google neither published the list of de-listed sites nor notified the owners of the de-listed sites of their actions. However, when a user performs a search for which all or part of the results are censored, Google.cn displays an explanation at the bottom of the screen that reads, "These search results are not complete, in accordance with Chinese law and regulations."

Google Senior Policy Council Andrew McLaughlin argued that by posting this warning, Google was providing the same level of transparency that it does for users in France, Germany and the U.S.[75] On Google.com in the U.S., results are often removed due to "cease and desist" requests resulting from copyright violations, but U.S. users are both alerted to the removal and provided with a link to read the complaint that resulted in the removal. French and German users also receive similar warnings with links to the actual complaint. In contrast, Chinese users are not advised about the number of results removed from the search or the complaints that resulted in the removal.

---

[72] Lindsay Eastwood, *"Don't Be Evil": Google Faces the Chinese Internet Market and the Global Online Freedom Act of 2007,* 9 Minn. J.L. Sci. & Tech. 287 (2008)
[73] Ibid.
[74] Clive Thompson, "Google's China Problem," *New York Times Magazine*. Quoted in "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch*. August 9, 2006. (retrieved October 10, 2010).
[75] "Google in China," *Google Blog*. Quoted in "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch*. August 9, 2006. (retrieved October 10, 2010).

In his testimony before the House of Representatives, Google VP Eliot Schrage announced that Google.cn would provide a link to the uncensored version of Google.com, in an effort to ensure that the uncensored version remains as available as possible to Chinese users. He also pointed out that Google only provides basic search services and map services through its Chinese language site. Other Google products that collect user data, including Gmail and Google blogging services, "will be introduced only when we [Google] are comfortable that we can provide them in a way that protects the privacy and security of users' information.[76]" Schrage also called for a greater role to be played by the U.S. government in the process, possibly by including the issue of free expression in bilateral or multilateral negotiations involving the Chinese government.

It is worth noting that in Google's case, popular sentiment has often indicated that blockages of Google in China result in competitive gains for Baidu, the leading homegrown Chinese search engine. Baidu.com, which was launched in 2002, leads the search industry in Chinese internet searches and is one of the most popular websites in the world. In 2007, statistics showed that Baidu attracted 52% of Chinese Internet search users, with Google the next closest at 33%. Whenever Google's Chinese search engine is blocked by Chinese censors, users who typically utilize Google will often switch to using Baidu.[77] In the opinion of industry experts, Google's decision to establish Google.cn was an attempt to cut into Baidu's rapidly increasing dominance of the Chinese market.[78] When this issue is seen as creating a clear

---

[76] "Testimony of Google Inc. before the Subcommittee on Asia and the Pacific, and the Subcommittee on Africa, Global Human Rights, and International Operations" given by Eliot Schrage, vice president, Global Communications and Public Affairs, Google Inc., U.S. House of Representatives Committee on International Relations, Joint Hearing: "The Internet in China: A Tool for Freedom or Suppression?" February 15, 2006, http://wwwa.house.gov/international_relations/109/sch021506.pdf, and http://googleblog.blogspot.com/2006/02/testimony-internet-in-china.html (both retrieved November 6, 2010).

[77] Lindsay Eastwood, *"Don't Be Evil": Google Faces the Chinese Internet Market and the Global Online Freedom Act of 2007,* 9 Minn. J.L. Sci. & Tech. 287 (2008)

[78] Ibid

competitive disadvantage for a foreign company, it may be reasonable for Google to request the assistance of the U.S. Trade Representative in raising the issue in the appropriate forums, possibly including the World Trade Organization.[79]

In 2008, Chinese dissident Guo Quan threatened to sue Google for censoring his name on their Chinese search engine without a legal basis. Quan claimed that the censorship was costing him business at his garment company (as noted above, in the Yahoo! case study.) However, unlike Yahoo!, Google stopped censoring Quan's name once the story broke in the media, and Quan dropped the threat of a lawsuit.[80]

In early 2010, Google revealed on its blog that it had been victim of a cyberattack originating in China.[81] The attack, codenamed Operation Aurora, had been aimed at a number of organizations, including Google, Adobe Systems, Yahoo!, Northrop Grumman, and Dow Chemical. The aims of the attacks, which occurred during the latter half of 2009, were to collect information about political dissidents, as well as to steal weapons information and software source code (which could then be used to develop computer viruses).[82]

Google claimed that some of its intellectual property had been stolen as a result of the attack. In addition, Google also suggested that the people behind the attack had attempted to access the Gmail accounts of Chinese political dissidents. Two separate Gmail accounts belonging to political dissident Ai Weiwei had been hacked into, although the hackers' accessibility was limited to reading email subject lines and finding the creation date of each

---

[79] Tim Wu, *Legal Implications of a Rising China: The World Trade Law of Censorship and Internet Filtering,* 7 Chi. J. Int'l L. 263 (2006)
[80] Elinor Mills. "Yahoo Sued by Chinese Dissidents Again." *CNet News.* February 27, 2008. http://news.cnet.com/8301-10784_3-9881042-7.html (retrieved November 8, 2010)
[81] David Drummond. "A new approach to China." *The Official Google Blog."* January 12, 2010. http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (retrieved October 30, 2010)
[82] Kelly Jackson Higgins. "'Aurora' Attacks Still Under Way, Investigators Closing In On Malware Creators." *Dark Reading Tech Center.* February 10, 2010. http://www.darkreading.com/vulnerability-management/167901026/security/attacks-breaches/222700786/index.html (retrieved November 8, 2010)

account.[83] Weiwei's bank accounts were also investigated by Chinese state security agents who claimed that Weiwei was under investigation for "unspecified suspected crimes.[84]" Other Gmail accounts belonging to Chinese political dissidents in Europe, Asia, and the U.S. had been accessed through various fishing and malware attacks.[85]

In its blog post, Google declared that it was reevaluating its decision to conduct business in China. Google stated that it planned to operate an uncensored version of its Chinese search engine "within the law, if at all," and was prepared to leave China if this was not possible. On the same day, Secretary of State Hillary Clinton issued a brief statement which condemned the attacks and compared Chinese Internet censorship to the Berlin Wall. Clinton also requested an official response from the Chinese government to Google's allegations.[86] The U.S. Congress announced plans a day later to investigate Google's claims.[87] The official Chinese media later stated that the incident was part of a U.S. government conspiracy.[88]

Google followed up on its claim to turn off the filtering on Google.cn, although the filtering was later re-enabled without any comment or explanation. In late March, Google began redirecting all visitors to its Google.cn site to its unfiltered Google Hong Kong search engine. Chinese officials strongly objected to the move, stating that it violated Google's "written

---

[83] Drummond. "A new approach to China." For identification of the accounts as belonging to Ai Weiwei see Jamil Anderlini. "The Chinese dissident's 'unknown visitors'". *Financial Times*, 15 January 2010 (retrieved November 7, 2010). http://www.ft.com/cms/s/0/c590cdd0-016a-11df-8c54-00144feabdc0.html.

[84] Anderlini. "The Chinese dissident's 'unknown visitors,'"

[85] Drummond. "A new approach to China."

[86] Hillary Rodham Clinton. "Statement on Google Operations in China." *U.S. State Department.* January 12, 2010. http://www.state.gov/secretary/rm/2010/01/135105.htm (retrieved November 3, 2010)

[87] Tom Ramstack. "Congress to Investigate Google Charges of Chinese Internet Spying." *All Headline News.* January 13, 2010. http://www.allheadlinenews.com/articles/7017511426?Congress%20to%20Investigate%20Google%20Charges%20Of%20Chinese%20Internet%20Spying (retrieved November 7, 2010)

[88] Katherine Hille. "Chinese media hit at 'White House's Google.'" *Financial Times*. January 20, 2010. http://www.ft.com/cms/s/e6022fe0-05c6-11df-88ee-00144feabdc0,Authorised=false.html (retrieved November 7, 2010)

obligations.[89]" In mid-2010, Google finally shut down its Chinese search engine, although it still maintains sales and research & development offices in China.[90] In late November 2010, Google released a white paper claiming that China's restrictions on the free flow of information violate WTO rules on free trade in services.[91] In their report to Congress released days after Google's white paper, the U.S.-China Economic and Security Review Commission acknowledged Google's views and recommended "that Congress urge the administration to pursue in international fora better protections of information on the Internet in order to facilitate trade.[92]"

Part II: Case Studies: Cisco Systems, Inc.

Cisco's involvement in the Chinese Internet censorship regime is distinctly different from that of the other companies mentioned before. Instead of offering Internet-based content and services to Chinese users, Cisco, along with several other U.S. companies, has sold both filtering software and hardware to the Chinese government, ISPs, and other customers within the Chinese market.[93] These routers can then be programmed to filter or block certain keywords or websites that users are attempting to access. By supplying the Chinese government with these crucial goods, U.S. companies are assisting in the creation and maintenance of the Chinese Internet censorship infrastructure.[94]

---

[89] David Barboza and Miguel Helft. "Google to Redirect China Users to Uncensored Site." *New York Times.* March 22, 2010. http://www.nytimes.com/2010/03/23/technology/23google.html (Retrieved November 13, 2010).
[90] Joe McDonald. "Google defends shrinking China market share." *Google News*. The Associated Press, 20 Sep 2010. Web. 10 Oct 2010. http://www.google.com/hostednews/ap/article/ALeqM5gwIr5_cMUInvCi4gjbSAW2tFpV6wD9IBIHMO0.
[91] "Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information." *Google*. http://docs.google.com/viewer?url=http://www.google.com/googleblogs/pdfs/trade_free_flow_of_information.pdf&chrome=true (retrieved November 23, 2010)
[92] Andy Greenberg. "Congress Commission Echoes Google: China's Censorship is Trade Barrier." *Forbes*. November 18, 2010. http://blogs.forbes.com/andygreenberg/2010/11/18/congress-commission-echoes-google-chinas-censorship-is-trade-barrier/?boxes=Homepagechannels (retrieved November 23, 2010)
[93] Jill R. Newbold, *Aiding the Enemy: Imposing Liability on U.S. Corporations For Selling China Internet Tools to Restrict Human Rights,* 2003 U. Ill. J.L. Tech. & Pol'y 503 (2003).
[94] Ibid

A leaked internal document from 2002 indicates that Cisco viewed sales of routers to the Chinese government as a business opportunity. The document discusses a Chinese government project, referred to as "Golden Shield," that was designed to expand the Chinese Internet censorship infrastructure. In the document, Cisco's Chinese employees discussed the opportunity to sell new Cisco routers to the Chinese government to assist in the project. One slide within the document discusses the Chinese government's announcement of the project's goals, which include "Combat[ing] Falun Gong evil religion and other hostiles [sic].[95]" Cisco would eventually sell around $100,000 worth of routers and other hardware to the Chinese government as part of the project. This amount dwarfs the $500 million per year that some experts estimate that Cisco earns in China.[96]

Once the document was leaked, human rights groups and lawmakers chastised Cisco for selling hardware that was being used to repress free speech on the Internet. Arvind Ganesan, a director at the Human Rights Watch, suggested that "if you know ahead of time that a sale could lead to human rights violations, and there's no way of mitigating that, maybe you shouldn't offer it to that entity." Cisco defended itself once the document was leaked, stating that the excerpt discussing the Falun Gong did "not represent Cisco's views…[and] were merely inserted in that presentation to capture the goals of the Chinese government in that specific project.[97]"

However, Cisco's entanglement in Chinese Internet censorship is not limited to the sale of hardware devices. The company is also suspected of providing training for Chinese engineers in how to use Cisco's products to censor Internet content.[98] Appearing before the House of

---

[95] Sarah Lai Stirland. "Cisco Leak: 'Great Firewall' of China Was a Chance to Sell More Routers." *Wired.* May 20, 2008. http://www.wired.com/threatlevel/2008/05/leaked-cisco-do/ (retrieved November 19, 2010)
[96] Christopher Stevenson, *Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World,* 30 B.C. Int'l & Comp. L. Rev. 531 (2007)
[97] Stirland. "Cisco Leak: 'Great Firewall' of China Was a Chance to Sell More Routers."
[98] The Internet in China: A Tool for Freedom or Suppression?: J. Hearing Before the Subcomm. on Africa, Global Human Rights and International Operations and the Subcomm. on Asia and the Pacific of the Comm. On

Representatives, Cisco Senior VP Mark Chandler claimed that "Cisco does not customize or develop specialized or unique [filtering] capabilities, in order to enable different regimes to block access to information.[99]" Later in his testimony, Chandler acknowledged that routing devices can be used for both security and censorship purposes, and Cisco sells their devices to China with the knowledge that they may be used for censorship purposes.

Why is Cisco's knowledge and intent in selling their devices important? Like many other forms of technology hardware, a router falls under the definition of "dual-use" technology. A router can be used for peaceful purposes (protecting a network from computer viruses) or for censorship and information repression. Like many nations, the U.S. sets limits on what technology can be exported by U.S. companies—including strong encryption technologies. Although the most restrictive trade terms are in place for notorious regimes such as Iran and China, technology-specific embargoes do exist on a number of nations, including China.

One of Cisco's products that China has purchased is Policenet, a crime prevention system that is used by police forces for quick retrieval of data on an individual. In testimony before the House of Representatives, Ethan Gutmann, a former business consultant in China, alleged that Cisco had sold Policenet to the Chinese state security forces. Gutmann quoted a Cisco engineer who stated that Policenet enabled a policeman to stop a Chinese citizen on the street, scan the citizen's ID card, and remotely access a treasure trove of information on the citizen, including the citizen's Internet browsing history for the last 60 days. As a result, Gutmann claimed that Cisco's technology aided in the arrests of political dissidents and other groups whose online

---

International Relations H.R., 109th Cong. 157 (2006), available at http://www.foreignaffairs.house.gov/archives/109/26075.pdf (statement by Lucie Morillon, Washington Representative, Reporters Without Borders).

[99] The Internet in China: A Tool for Freedom or Suppression? at 77-80 (statement of Mark Chandler, Senior Vice President and General Counsel, Cisco Systems, Inc.).

speech has been repressed.[100] If Gutmann's allegations are true (which Cisco has denied), Cisco may have run afoul of U.S. export law prohibiting the export of "identification retrieval technologies" to China.[101]

At the time of this paper's writing, Cisco Systems maintains 12 separate offices within China, according to its website.[102] Despite the criticism over its role in supplying critical pieces to China's Internet censorship infrastructure, Cisco has not publicly acknowledged any wrongdoing and recently pledged "hundreds of millions of dollars" to build up its business presence in China.[103]

Part III: Potential Solutions: Alien Tort Claims Act

The Alien Tort Claims Act (ATCA) dates back to 1789, when it was first enacted as part of the Judiciary Act. Although the ATCA was seldom used over the first two centuries of its existence, it has seen a recent surge in interest due to the global activities of U.S. companies and the impact of their actions on foreign citizens.[104] The ATCA gives federal district courts in the U.S. subject matter jurisdiction over "civil actions by an alien for tort only, committed in violation of the law or nations or a treaty of the United States.[105]" The ATCA has been

---

[100] Tom Espiner. "Amnesty Condemns Tech Firms Over Human Rights." *ZDNet UK*. June 1, 2006. http://www.zdnet.co.uk/news/security-management/2006/06/01/amnesty-condemns-tech-firms-over-human-rights-39272429/ (retrieved November 19, 2010).

[101] 15 C.F.R. § 774, Supp. 1, ECCN no. 3A981 (2008) (identifying "automated fingerprint and identification retrieval systems" as controlled for crime control reasons under the Export Administration Regulations(EAR))

[102] "Asia/Pacific Sales Offices." *Cisco Systems*. http://www.cisco.com/web/siteassets/contacts/offices/asiapac.html (retrieved November 7, 2010).

[103] Tania Branigan. "We're staying in China, says Microsoft, as free speech row with Google grows." *The Guardian.* March 25, 2010. http://www.guardian.co.uk/technology/2010/mar/25/china-microsoft-free-speech-google (retrieved November 7, 2010)

[104] DeNae Thomas, *Xiaoning v. Yahoo! Inc.'s Invocation of the Alien Tort Statute: An Important Issue but an Improper Vehicle*, 11 Vand. J. Ent. & Tech. L. 211 (2008)

[105] 28 U.S.C. § 1350

successfully utilized by victims of human rights abuses to sue both state officials and multinational corporations in U.S. courts.[106]

The most notable instance of the ATCA in Supreme Court jurisprudence is from *Sosa v. Alvarez-Machain*, where a Mexican alien sued a Mexican national under the ATCA for abducting him in Mexico and delivering him to U.S. authorities, who then arrested him for the murder of a federal agent.[107] In its ruling, the Supreme Court stated that the ATCA is solely a jurisdictional grant, and does not supply a cause of action. Instead, a cause of action must come from within the "law of nations," which the Court defined as customary international law or treaties to which the United States is a party. The Court limited these causes to a "narrow class" of international norms that have been "accepted by the civilized world." Included within this "narrow class" are torture, extrajudicial killings, and some forms of prolonged arbitrary detention.[108]

Therefore, the simple act by an ICT of divulging user information to another party is not grounds for a cause of action according to the precedent laid by *Sosa*. Instead, an ICT must provide the information to a state actor—an ICT acting alone would not be cause for an ACTA suit. In addition, the information must be given "with the knowledge that the state intends to use the information to commit human rights violations.[109]" Doing so opens an ICT up to liability on the grounds of "aiding and abetting human rights violations committed by states.[110]"

---

[106] See, e.g., *In re Estate of Marcos*, 25 F.3d 1467 (9th Cir. 1994) (ATCA suit against the former President of the Philippines), *Khulumani v. Barclay Nat'l Bank Ltd.*, 504 F.3d 254 (2d Cir. 2007) aff'd without opinion, 128 S. Ct. 2424 (2008) (ATCA suit against banks for aiding and abetting Apartheid in South Africa).
[107] 542 U.S. 692 (2004).
[108] See Restatement (Third) of Foreign Relations Law of the United States § 702 (1987) ("A state violates international law if, as matter of state policy, it practices, encourages or condones...(c) murder...(d) torture...(e) prolonged arbitrary detention...").
[109] Brian R. Israel, *"Make Money Without Doing Evil?" Caught Between Authoritarian Regimes in Emerging Markets and a Global Law of Human Rights, U.S. ICTs Face a Twofold Quandry,* 24 Berkeley Tech. L.J. 617 (2009)
[110] Ibid

Although precedent clearly shows that corporations can, and have been, held liable for aiding and abetting international law violations, the standard for what constitutes aiding and abetting has been somewhat murkier. In *John Doe I v. Unocal Corporation*, the Ninth Circuit Court of Appeals upheld an earlier ruling that corporations could be held liable as accessories to human rights abuses under the ATCA. The majority opinion drew inspiration for their standard from international law, mainly the International Criminal Tribunals for the Former Yugoslavia and Rwanda. The decision stated that aiding and abetting liability could be imposed for "knowing practical assistance or encouragement which has a substantial effect on the perpetration of the crime.[111]" But a concurring opinion on the same case, authored by Judge Reinhardt, urged federal judges to "look to traditional civil tort principles" in judging accessorial liability.[112] Another recent case, *Khulumani v. Barclay Nat'l Bank Ltd.,* showed a similar disagreement between the authors of the concurring opinions over the source of a standard for aiding and abetting.[113] However, the source of the standard is of diminished importance for multinational IT corporations, as the sole difference between the two lies in whether the company merely has knowledge of the state actor's intentions or acts with the purpose of facilitating them.

The ATCA reemerged as part of the censorship controversy due to the cases of Shi Tao and Wang Xiaoning, two Chinese dissidents who were allegedly imprisoned as a result of Yahoo!'s cooperation with Chinese authorities. In 2005, both Tao and Xiaoning were arrested

---

[111] *John Doe I v. Unocal Corporation*, 395 F.3d at 947. Judge Pregerson, the author of the majority opinion, derived this standard principally from the ICTY's decision in Prosecutor v. Furundzija, IT-95-17/1-T (Dec. 10, 1998), reprinted in 38 I.L.M. 317 (1999).

[112] *Unocal*, 395 F.3d at 965 (Reinhardt, J., concurring).

[113] *Khumulani v. Barclay Nat'l Bank Ltd.,* 504 F.3d 254, 256 (2d Cir. 2007). In the case, the judges authoring the concurring opinions differed over whether the evaluation of "aiding and abetting" liability should be based on international or federal law. See Khurram Nasir Gore, *Xiaoning v. Yahoo!: Piercing the Great Firewall, Corporate Responsibility, and the Alien Tort Claims Act,* 27 Temp. J. Sci. Tech. & Envtl. L. 97 (2008). For case description, see footnote 100.

by Chinese authorities after Yahoo! supplied the Chinese government with personal identification information for both individuals following a request by the Chinese government. According to the lawsuits (which were filed independently and later combined), both men were subjected to prolonged arbitrary detention and torture at the hands of Chinese law enforcement. Each filed suit against Yahoo! Hong Kong (the entity that allegedly supplied the information) and Yahoo! Inc. in the United States, accusing them of "aiding and abetting" human rights violations by the Chinese government.

Although the case was settled out of court before going to trial, the facts still represent a likely scenario under which a U.S. IT company could be held liable under the ACTA. The plaintiffs' success in proving their allegations of arbitrary detention and torture would have fulfilled the requirements of the ACTA for "state action" that violates international norms. If the courts had applied the knowledge standard (under which Yahoo! would merely have had to have known of China's intent in using the information), the plaintiffs could have pointed to Yahoo!'s handover of personal information that enabled the Chinese authorities to identify and arrest the plaintiffs. The question of liability would have then centered on Yahoo!'s knowledge of China's intent in procuring the information.[114] The plaintiffs would have had to prove that Yahoo! knew that political dissidents arrested in China would likely face prolonged arbitrary detention and possible torture—an uphill battle, but a winnable one given the amount of press and exposure that has been dedicated to human rights abuses in China.[115]

Conversely, under the purposefulness standard (Yahoo! intended to facilitate acts of torture by handing over the user information), Yahoo! would have likely escaped liability.

---

[114] Mara D. Bryne, *When in Rome: Aiding and Abetting in Wang Xiaoning v. Yahoo*, 34 Brooklyn J. Int'l L. 151 (2008)

[115] Ibid. In his testimony before Congress, Yahoo! General Counsel Michael Callahan admitted that the request for information relating to Shi Tao did contain reference to an investigation for disclosure of "state secrets." Crimes relating to "state secrets" are widely known to be political in nature in China.

Although the plaintiffs could have argued that Yahoo! knew that China intended to prosecute them for various politically motivated crimes, that would not have proven that Yahoo! intended to facilitate human rights abuses by the Chinese government. Most successful findings thus far against companies under the purposefulness standard have concerned corporations conspiring with state governments to protect their physical assets in that state, and it is highly unlikely that an IT company would find itself in such a situation.[116]

Although the ACTA presents a viable option for foreigners injured by the actions of U.S. IT companies overseas, its applicability is narrow, and the chances of a finding of liability are slim. Since multinational corporations almost never directly violate international laws and norms, a suit against a multinational corporation under the ACTA would likely concern the "aiding and abetting" of the violation of international law and norms by a multinational corporation.[117] An IT company would have to be caught red-handed in the course of "aiding and abetting" human rights abuses in order to be held liable under the ACTA, a scenario unlikely to unfold. While Yahoo! may have escaped liability had the case gone to trial, the bad press that the company received during the trial—and their subsequent decision to settle the case—left many observers with a negative impression of the company.[118] This negative publicity may have been the biggest impact of the ACTA on IT policy in China, as other U.S. companies took note of the waves of negative publicity directed at Yahoo! both during and following the suit.

---

[116] *Unocal, 395 F.3d. 932* (9th Cir. 2002) (Burmese villagers alleged murder, rape, torture and forced labor in connection with the construction of a gas pipeline); *Bowoto, 2006 U.S. Dist. LEXIS 63209* (N.D. Cal. 2006) (Involving human rights violations committed by Nigerian security forces against protesters on a Chevron oil platform).

[117] Mara D. Bryne, *When in Rome: Aiding and Abetting in Wang Xiaoning v. Yahoo*, 34 Brooklyn J. Int'l L. 151 (2008)

[118] Khurram Nasir Gore, *Xiaoning v. Yahoo!: Piercing the Great Firewall, Corporate Responsibility, and the Alien Tort Claims Act,* 27 Temp. J. Sci. Tech. & Envtl. L. 97 (2008)

Part III: Potential Solutions: Global Online Freedom Act

The Global Internet Freedom Act is a bill introduced in 2009 by Representative Chris Smith (R-NJ) that seeks to impose punishments on U.S. companies that share user data with "Internet-restricting" countries. The bill (HR 2271) was originally introduced in 2007, but failed to gain traction.[119] A similar bill had been previously introduced in 2005 by Smith, under the title of "Global Internet Freedom Act.[120]" The current bill was referred to the Subcommittee on Commerce, Trade and Consumer Protection in May 2009.[121]

According to a summary of the bill by the Congressional Research Service, the Global Online Freedom Act has the following three policy goals:

1. Promote the freedom to seek, receive, and impart information and ideas through any media;
2. Use all appropriate instruments of U.S. influence to support the free flow of information without interference or discrimination; and
3. Deter U.S. businesses from cooperating with Internet-restricting countries in effecting online censorship.[122]

In order to meet these three objectives, the Act would begin by creating an Office of Global Internet Freedom (OGIF) within the Department of State, as well as obligating the Secretary of State to annually designate a list of Internet-restricting countries. The Office of Global Internet Freedom, hailed by one expert as "the most significant and enduring" provision of the Act,

---

[119] Roy Mark. "Google, China Dispute Revives Global Online Freedom Act." *eWeek.* January 17, 2010. http://www.eweek.com/c/a/Government-IT/Google-China-Dispute-Revives-Global-Online-Freedom-Act-493296/ (retrieved November 18, 2010).
[120] Nellie L. Viner, *The Global Online Freedom Act: Can U.S. Internet Companies Scale the Great Chinese Firewall at the Gates of the Chinese Century?,* 93 Iowa L. Rev. 361 (2007)
[121] Congressional Research Service. "Summary: Global Online Freedom Act of 2009." *Govtrack.* http://www.govtrack.us/congress/bill.xpd?bill=h111-2271&tab=summary (retrieved November 15, 2010)
[122] Ibid

would become the government hub for data collection related to internet censorship.[123] U.S. businesses that collect users' personal information would be required to notify the OGIF before responding to a disclosure request from a foreign government. Additionally, U.S. businesses that create, provide, or offer "to the public for commercial purposes an Internet search engine or…Internet communications services or Internet content hosting services" would be prohibited from locating any personal information within an Internet-restricting country.[124]

The Act also included a push for greater transparency by requiring U.S. companies to disclose their lists of filtered keywords or websites to the OGIF. In addition, U.S. companies could be subject to civil penalties of up to $2 million for violating the Act. The penalties section also covered liability of U.S. companies for actions of foreign entities, which would occur if the U.S. company

1) Controls a controlling interest in voting shares or other equity securities of the foreign entity;
2) Authorizes, directs, controls, or participates in the acts by the foreign entity; or
3) Authorizes, in whole or in part, by license or otherwise, the foreign entity to use the trade name of the United States business in connection with goods or services provided by the foreign entity.

In addition to the penalties for corporations, any individual who provides a foreign government official with information in violation of the Act would face a fine and up to five years in prison.[125]

---

[123] William J. Cannici, Jr., *The Global Online Freedom Act: A Critique of Its Objectives, Methods, and Ultimate Effectiveness Combating American Businesses That Facilitate Internet Censorship in the People's Republic of China,* 32 Seton Hall Legis. J. 123 (2007).
[124] Ibid
[125] Congressional Research Service. "Summary: Global Online Freedom Act of 2009." *Govtrack.* http://www.govtrack.us/congress/bill.xpd?bill=h111-2271&tab=summary (retrieved November 15, 2010)

The Global Online Freedom Act is a laudable attempt at attempting to regulate the dealings of U.S. IT companies with China. By preventing these companies from housing user information on servers located in China, the Act would move this information out of the reach of Chinese legal authorities. The imposition of fines and prison sentences for violating the Act's prohibitions on information disclosure should be a satisfactory deterrent to the kind of cooperation with law enforcement that Yahoo! engaged in.[126] Even if companies are still required to engage in some forms of censorship, the Act's disclosure provisions would create increased transparency.[127] Additionally, the Act's inclusion of foreign subsidiaries and other foreign actors as entities that could create liability through their actions could prevent many U.S. companies from following in Yahoo!'s footsteps and partnering with a Chinese company in an attempt to create plausible deniability.

However, on a pragmatic level, the Act does stop short of a complete solution. Although the Act requires disclosure of blocked terms and de-listed websites, these websites can simply be blocked by China at the ISP and IAP levels. Losing the cooperation of U.S. MNCs would be a blow to Chinese censorship efforts, but China was previously able to significantly reduce the effectiveness of Google.com for Chinese users without any cooperation on Google's part. In addition, Google cited the ineffectiveness of Google.com for Chinese users as a significant factor in their decision to enter the Chinese market. Although China could no longer legally access user data if it is no longer stored on servers within China, it could make accessing servers outside of China painfully difficult for Chinese Internet users.[128] The Act's provisions do nothing to prevent the activities of a corporation, such as Cisco, that sells hardware and provides technical

[126] Nellie L. Viner, *The Global Online Freedom Act: Can U.S. Internet Companies Scale the Great Chinese Firewall at the Gates of the Chinese Century?,* 93 Iowa L. Rev. 361 (2007)
[127] Ibid
[128] Ibid

support in Internet-repressing countries. Legal experts have also expressed concern that the Act would be seen as "exporting" American values of free speech and seeking to force them on other countries, and have urged the consideration of multilateral approaches instead.[129]

If passed into law, the Act may run into a First Amendment challenge based on precedent from the Supreme Court case *West Virginia State Board of Education V. Barnette*. In *Barnette*, the Court held that the Constitution protects both the freedom to speak and the freedom not to speak.[130] The Act's prohibition of censorship would force search engine companies to display all results regardless of their wishes, which may arguably violate the precedent of *Barnette*. However, the Court recently ruled in *Rumsfeld v. Forum for Academic and Institutional Rights* that institutions serving the public (such as search engines) 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.[131] If the Act was passed into law and challenged on First Amendment grounds, legal experts believe that *Barnette*'s protection of the right not to speak would likely be outweighed by *Rumsfeld*. Since search engines would likely not be seen as endorsing the results that they display, they could be compelled to use their online "facilities" for speech that they may not agree with.[132]

The entire debate surrounding the Act may be a moot point. It has been stuck in committee since May 2009, and even an uproar surrounding Google's decision to leave China has failed to jolt it forwards. The critical mass of U.S. legislative support for such action has not

---

[129] Nellie L. Viner, *The Global Online Freedom Act: Can U.S. Internet Companies Scale the Great Chinese Firewall at the Gates of the Chinese Century?,* 93 Iowa L. Rev. 361 (2007)
[130] *West Virginia State Board of Education v. Barnette,* 319 U.S. 624 (1943)
[131] *Rumsfeld v. Forum for Academic and Institutional Rights, Inc.*, 547 U.S. 47 (2006)
[132] Marc D. Nawyn, *Code Red: Responding to the Moral Hazards Facing U.S. Information Technology Companies in China,* 2007 Colum. Bus. L. Rev. 505 (2007)

yet been achieved, and any action taken by the U.S. government in the meantime may have to occur within trade negotiations or one of several multilateral arenas.[133]

Part III: Potential Solutions: UN Global Compact

The UN Global Compact is an initiative undertaken by a diverse array of private and public stakeholders, led by the UN, to promote corporate social responsibility. Originally launched in 2000, the Compact featured nine principles, covering human rights, labor, and the environment.[134] A tenth principle (anti-corruption) was added during the Global Compact Leaders Summit in 2004.[135] The ten principles are derived largely from the Universal Declaration of Human Rights, as well as various other UN treaties on labor rights and corporate responsibility.

The Global Compact is not enshrined within the statutory law of signatory nations, but instead enacted by signatory corporations in the form of a voluntary code of conduct or a similar expression of support for ethical business practices. In order to participate, "the CEO of an organization must send a letter to the U.N. Secretary General expressing support for the Global Compact and its principles.[136]" In addition, the corporation is expected to implement changes in the manner in which it conducts business in order to comply with the Compact, in addition to publishing an annual account of the steps it has taken to comply.[137]

---

[133] Lindsay Eastwood, *"Don't Be Evil": Google Faces the Chinese Internet Market and the Global Online Freedom Act of 2007,* 9 Minn. J.L. Sci. & Tech. 287 (2008)
[134]"Guide to the Global Compact: A Practical Understanding of the Vision and Nine Principles." *Association for Sustainable & Responsible Inv. in Asia.* http://www.asria.org/ref/library/csrguidelines/lib/gcguide.pdf (retrieved November 20, 2010)
[135] Global Compact Office, Preliminary Report on the Global Compact Leaders Summit 1 (2004), available at http://www.pactoglobal.org.br/doc/summit%20report.pdf. The tenth principle states that "Businesses should work against all forms of corruption, including extortion and bribery."
[136] Surya Deva, *Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?*, 39 Geo. Wash. Int'l L. Rev. 255 (2007)
[137] Ibid

In the arena of Internet censorship, the two most important of the ten principles are the first two, which cover human rights. The first principles states that "[b]usinesses should support and respect the protection of internationally proclaimed human rights." The second principle states that "[businesses should] make sure that they are not complicit in human rights abuses.[138]" One can safely assume that since most UN documents concerning human rights (including the International Covenant on Civil and Political Rights) discuss the freedom of speech and expression in all media, such a right would be covered under the first principle of the Global Compact. Assuming this, the second principle would directly implicate the four companies discussed thus far as "complicit in human rights abuses" by assisting in the political censure of Internet speech in China.

However, those hoping to hold businesses accountable for their actions in China will be disappointed by the Global Compact's lack of regulatory teeth. The Compact states that it "is not a regulatory instrument—it does not 'police,' enforce or measure the behavior or actions of companies.[139]" The Compact even resists being categorized as a benchmarking system on which to measure the relative ethical performance of companies, instead insisting in being categorized as a "learning dialogue and platform of action" for the participating companies[140].

Over the years, the number of participants in the Global Compact has increased drastically, from 38 in July 2000 to over 6,000 in 2010.[141] However, the number of participants is a hollow measure of the Compact's effect, as the lack of enforcement and accountability

---

[138] "The Ten Principles." *United Nations Global Compact.* http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/index.html (retrieved November 10, 2010).
[139] "What is the Global Compact?" *United Nations Global Compact.* http://www.unglobalcompact.org/AboutTheGC/index.html (retrieved November 12, 2010).
[140] Interview by PriceWaterhouseCoopers with Georg Kell, Executive Head, Global Compact (2005). Available at http://www.unglobalcompact.org/docs/news events/9.5/pwc int 2005.pdf (retrieved November 2, 2010).
[141] UN Global Compact: 2010 Annual Review. http://www.unglobalcompact.org/docs/news_events/8.1/UNGC_Annual_Review_2010.pdf (retrieved November 22, 2010).

mechanisms limits the Compact's effectiveness. Cisco Systems, for instance, is a signatory to the Global Compact, but has continued to supply the Chinese government with routers for Internet censorship in direct violation of the Compact's second principle.[142] Microsoft, another member of the compact, has actively participated in Chinese censorship.[143] The lack of accountability of signatories to the Compact makes it easy for companies who have pledged their support to violate its principles, and limits its effectiveness as an effort to promote increased corporate social responsibility.

Part III: Potential Solutions: International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR) was adopted by the UN General Assembly in 1966 and entered into force in 1976. The multilateral treaty is centered on the recognition of various civil and political rights of individuals, including freedom of speech and freedom of expression. The treaty, and the compliance of the signatory bodies, is monitored by the Human Rights Committee, which reviews regular reports of the signatory states on the implementation of the rights guaranteed by ICCPR. The reports are usually submitted every four years. As of October 2009, the treaty had 72 signatories, including the United States. Although China has signed the ICCPR, it has yet to ratify it.[144] Hong Kong, however, has both signed and ratified the treaty.[145]

For those concerned with censorship of speech and expression on the Internet, the most relevant part of the ICCPR is found in Article 19, which covers the "right to freedom of

---

[142] Cisco Corporate Citizenship: UN Global Compact, http://www.cisco.com/web/about/ac227/about_cisco_corp_citi_global_compact.html (retrieved November 17, 2010).
[143] Surya Deva, *Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?*, 39 Geo. Wash. Int'l L. Rev. 255 (2007)
[144] Nellie L. Viner, *The Global Online Freedom Act: Can U.S. Internet Companies Scale the Great Chinese Firewall at the Gates of the Chinese Century?,* 93 Iowa L. Rev. 361 (2007)
[145] UN Treaty Collection: International Covenant on Civil and Political Rights. Available at http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en (retrieved November 10, 2010)

expression.[146]" Article 19(2) elaborates upon this right, which includes the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print…*or through any media*…(emphasis added).[147]" It goes without saying that in all of the cases covered above, individuals were imparting information and/or ideas through the Internet, with falls under the definition of "any media" within Article 19(2). Others sought to "receive…information" through searches on one of several search engines operating in China.

As China has yet to ratify the ICCPR, any violations that it may commit are of minimal impact. In addition, the absence of any enforcement measures and the presence of exceptions for national security and public order under the ICCPR limit its effectiveness.[148] Although the intent of the ICCPR was to enshrine the principles contained in the treaty within the law of each signatory nation, this has not yet become reality. Even in the United States, the treaty was ratified with five reservations, and previous cases have held that the ICCPR does not create a cause of action within U.S. courts.

However, the ratification of the ICCPR by Hong Kong, and its subsequent incorporation into the law of Hong Kong in 1991, does raise interesting questions. Many of the rights within ICCPR were incorporated, word for word, into the Hong Kong Bill of Rights.[149] In the court documents filed under ATCA by Xiaoning and Tao, both plaintiffs named Yahoo! of Hong Kong as a defendant, claiming that employees of Yahoo! in Hong Kong had provided Chinese authorities with information on both plaintiffs and their online activities.

---

[146] International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), art. 19, U.N. GAOR, 21st Sess., 1496th plen. mtg., U.N. Doc. A/6316 (Dec. 16, 1966) (hereafter "ICCPR")
[147] ICCPR art. 19(2).
[148] Kristen Farrell, *The Big Mamas Are Watching: China's Censorship of the Internet and the Strain on Freedom of Expression,* 15 Mich. St. J. Int'l L. 577 (2007)
[149] Chapter 383, Hong Kong Bill of Rights Ordinance 991. Available at http://www.hku.hk/law/conlawhk/sourcebook/10091.htm (retrieved November 2, 2010)

Could the plaintiffs have found a cause of action against Yahoo!'s employees in Hong Kong? The statutory law within Hong Kong's Bill of Rights is frustratingly unclear on this point, due to a "national security" exception.[150] Article 16(2) of the Bill of Rights repeats the ICCPR verbatim, guaranteeing "freedom to seek, receive and impart information and ideas of all kinds…through any…media of his choice.[151]" However, Article 16(3) outlines "certain restrictions" placed upon the rights outlined in Article 16(2). These restrictions, which were also contained in the ICCPR itself, include "the protection of national security or of public order (ordre public), or of public health or morals.[152]" In the case that Tao and Xiaoning had alleged a violation of Article 16(2), courts could have pointed to the restrictions contained in Article 16(3) as allowing Yahoo! employees to provide identifying information in the name of "national security" or "protection of…morals.[153]"

The promise of ICCPR, therefore, may be of little use in protecting political dissidents and other individuals from arrest and persecution by Chinese authorities. As the tenets of ICCPR have not been ratified by China, much less incorporated into Chinese law, they cannot be enforced within China. Even in Hong Kong, where they have been incorporated into a bill of rights, exceptions for "national security" and "morals" leave the government and employees of Western IT companies loopholes through which to escape liability for cooperation with Chinese censorship.[154]

---

[150] Anne Cheung and Rolf H. Weber, *Internet Governance and the Responsibility of Internet Service Providers,* 26 Wis. Int'l L.J. 403 (2008)
[151] Chapter 383, Hong Kong Bill of Rights Ordinance 991. Available at http://www.hku.hk/law/conlawhk/sourcebook/10091.htm (retrieved November 2, 2010)
[152] Ibid
[153] Cheung, *Internet Governance and the Responsibility of Internet Service Providers*
[154] Ibid

Conclusion

In Part II, this paper outlined the difficulties that U.S. IT companies have encountered when operating in China. They can be broadly divided into two different categories—those associated with content hosting, and those associated with search censorship. The content hosting issues have only been experienced to a large extent by Yahoo!, as the only one of the companies to host email and user data on servers located within China. As a result of their decision to locate the servers within China, Yahoo! China employees were compelled to turn over user data upon request from Chinese authorities—actions that led not only to the imprisonment of political dissidents, but several U.S. lawsuits and endless negative press. The solution to this problem, articulated by Microsoft and Google, is simple—do not physically locate user data within China. Both companies cited their reluctance to hand over user data as a key factor in their decision to not offer email services to Chinese users.

Search censorship is a harder issue to tackle, in part due to the lack of control of U.S. companies over this problem. Google's decision to withdraw from China showed that one company's efforts to stand up to China's censorship regime were futile, and Yahoo! and Microsoft have continued to filter their Chinese search engines (although both hold only small slivers of the Chinese market). However, Google's stand against China may have affected the thinking of other companies, as fellow Internet giants Facebook and Twitter have stated that they have no plans to develop a Chinese-language site or submit themselves to Chinese censorship of any sort.[155]

The legal remedies available to control the actions of these companies within China are lacking, to say the least. Although the ATCA does offer a viable route for imprisoned political

[155] Tania Branigan. "We're staying in China, says Microsoft, as free speech row with Google grows." *The Guardian.* March 25, 2010. http://www.guardian.co.uk/technology/2010/mar/25/china-microsoft-free-speech-google (retrieved November 7, 2010)

dissidents to seek damages from U.S. companies that played a role in their detention, the standard for proof is steep, and the statute would only take effect once the plaintiff has actually been injured by a U.S. company's actions (as opposed to serving as a deterrent for violations of human rights by U.S. companies). The Global Online Freedom Act of 2010 is a worthy legislative gesture, but is highly unlikely to become law anytime in the near future.

Multinational solutions offer no better solutions to the issue. ICCPR's Article 19, which covers freedom of expression on the Internet, would only take effect upon its incorporation into a nation's statutory law. While it has been incorporated into U.S. law, courts have agreed that it does not represent a cause of action for plaintiffs. China has signed onto the ICCPR, but has yet to ratify the treaty or incorporate it into its statutory law. The UN Global Compact, on the other hand, explicitly rejects any police measures that would keep companies in line. Cisco Systems' membership within the Compact, juxtaposed with its alleged violations of the Compact in China, show how the lack of enforcement mechanisms within the Compact are hurting its ability to achieve its goal of increased corporate social responsibility.

In the end, perhaps neither existing statutory law nor current multinational treaties are the answer. Human rights groups and NGOs are looking for ways to fight human rights abuses by Chinese authorities and U.S. companies before they happen, and no such deterrent currently exists (outside of negative public opinion, of course). Perhaps, as Google's latest statements suggest, the issue may have to be resolved as a matter of free trade on a multinational level. If pressure from other nations can force China to open up its cyberspace to foreign competition, then the "Great Firewall of China" may finally crumble to the ground.