China, Multinational Corporations, and Internet Privacy Issues: An Incoherent Landscape

Lysette Kent

Abstract

In the mid 2000s, staff at the Chinese division of Yahoo! sent information on one of its users, Shi Tao, to the Chinese government. The journalist had been critical of the Chinese government, and, based on the information sent to the government, Shi Tao was sentenced to ten years in prison. In 2010, e-mail accounts housed by Google were hacked. Many of these accounts belonged to human rights activists. Issues like these pose a conundrum for the United States and international entities that are looking to prevent human rights abuses, including violations of privacy, in countries such as China. This paper will evaluate current and proposed efforts to curb such actions by the Chinese government. I propose the following three-pronged approach to deal with these actions: 1) a vigorous naming, blaming, and shaming campaign; 2) the adoption of a uniform policy by the United States government for addressing the Chinese government on these issues; and 3) the development of coherent, enforceable, and specific codes of conduct by trade associations and business groups that discuss issues of censorship and privacy regarding the internet, their customers, and foreign governments.

Statement of the Problem

In the mid-2000s, staff at the Chinese branch of Yahoo! sent private information on one of its users, Shi Tao, to the Chinese government. Shi Tao was a journalist who had been critical of the Chinese government in e-mails on his Yahoo! account. Based on agreements that Yahoo! had entered into with the Chinese government in an effort to get access to a large, rapidly expanding market share in China, Yahoo! was not placed in control of such decisions. This is because they were required to enter into a partnership with China-based company Alibaba, in which the Chinese state still maintains a 40 percent stake.[1] Because of this, Shi Tao was arrested, tried, and sentenced to 10 years in prison for "e-mailing 'state secrets.'"[2] After this, Yahoo! was investigated by Congress for its role. Yahoo! provided the defense that they did not know the scope of the information being asked for by the Chinese government. They stated that the request was handled entirely by the Yahoo! China offices in Beijing.[3] This shows one type of privacy violation, in which a company provides information to the Chinese government, regarding the use of the internet by one of or a group of their customers. Other cases show different issues that arise involving privacy, the internet, and China. Considering these issues, this paper will attempt to address what the proper role of multinational corporations should be regarding foreign countries that impose unfair restrictions on the internet or use the internet to violate the privacy of their citizens. This paper will use China as a case study and will discuss, in detail, the Yahoo! case and the case of Google in 2010. With Yahoo! implicated in the Shi Tao case (amongst others) and other companies, such as Google, Cisco, and Microsoft implicated in corporate complicity regarding the censorship of the internet in China, this question is extraordinarily relevant in today's world. China has nearly 400 million people online, a number that has shown rapid growth in recent years and has the potential to more than double its number of internet users in the near future, making this question even more pressing.

Standing in contrast to the Yahoo! case is the case of Google. In 2010, Google left the Chinese market after experiencing a string of cyber attacks. According to Google's blog, they discovered that the attacks were meant to infiltrate the e-mail accounts of Chinese human rights activists.[4] Google attempted to reroute its services through its Google Hong Kong browser.[5] However, the Chinese government eventually stopped this service. Currently, the Google China website displays a page that will only lead to Google Hong Kong, a site that will not currently run searches.[6] Some have argued that Google's response sounded like "sour grapes from a company with a low market share, weak revenues, and unfair competition during its four years inside the Great Fire Wall."[7] Regardless of the differences between the Yahoo! case and the Google case, the Google case links these issues, showing how the Chinese censorship

1 Jeffrey G. MacDonald, "When Yahoo! in China is Not Yahoo!," *Christian Science Monitor* 98(55): 1-2.
2 Robert Marqueland, "Yahoo!, Chinese Police, and a Jailed Journalist," *Christian Science Monitor 97*(201): 7.
3 "Yahoo!'s Defense in Case of Jailed Dissident," *Business Week Online*, November 7, 2007, 18.
4 "A New Approach to China: The Official Google Blog, January 12, 2010," accessed May 31, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.
5 "A New Approach to China: The Official Google Blog, March 22, 2010," accessed May 31, 2010, http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html.
6 "Google China," accessed November 10, 2010, http://www.google.cn.
7 Jonathan Watts, "How Internet Giant Google Turned on Gatekeepers of China's Great Firewall," *The Guardian*, January 14, 2010.

regime can box a company in regarding issues of privacy.

In short, these two cases show that there are two types of privacy violations when it comes to the internet in China. There are those privacy violations that occur because a company turned information over to the government and those privacy violations that occur when hackers try to attack a company and get information. This paper will try to determine the proper role of multinational corporations, trade associations and business groups, international NGOs, and the international political community in addressing these issues. I will examine these two cases to more fully understand this difference between the types of violations and then will pose the policy implications for the international community throughout the paper. Thus, this paper will posit that such violations need to be met with a multifaceted approach that includes actions from governmental and nongovernmental organizations, as opposed to the current, purely legal, approach.

The first problem discussed will be situations in which a company provides information to a government. The problem in these situations is one of corporate complicity with authoritarian regimes as it relates to the internet. Violations of privacy by companies such as Yahoo! can have a deleterious effect on privacy rights, and proposed measures to stop these actions from occurring have been ineffective. The second problem concerns companies being raided by hackers to take information. In discussing this point, this paper will touch on the GhostNet hack and the Google situation in China in late 2009 and early 2010. Thus, there is another side of privacy violations, those without corporate complicity, and these could be considered equally dangerous. There are these two types of privacy violations, but the second type of violation could be of two characters: 1) the government did not have the appropriate leverage to get the information it wanted, or 2) there was a large amount of independent and non-governmental hackers within China that are bent on protecting the country's nationalism.

Some may argue that this difference makes the case of Google irrelevant in this paper, given that they were attacked to gain information, rather than comply with a request from the Chinese government. However, Google did have a past history of complying with Chinese government requests, providing a censored version of their search engine.[8] Thus, even though Google is not readily giving up information to the Chinese government, their history of corporate complicity (censoring their search engine in China) still makes this case relevant. It may just show the differences that arise between a company that has a well-established and governmentally backed presence in China (Yahoo! with Alibaba), versus the actions of an independent company (Google). This is especially important because it is not known if the Chinese government initially asked for information from Google before this string of cyber attacks or if the company was simply attacked. Thus, even with its differences, the case is important within the context of this paper.

8 Human Rights Watch, "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship," *Human Rights Watch 18*(8): 5.

Methodology

In discussing privacy issues in China, two recent cases exemplify the complex issues that surround the internet. These two cases involve two major multinational corporations, Yahoo! and Google. In approaching this subject, this paper will first discuss each case, the specific facts of each, and the major differences between them. Doing this will give a brief history of privacy issues, the internet, and multinational corporations in China, based on the limited history of the internet in China. The case involving Yahoo! occurred in 2006 and the case concerning Google occurred in 2010. While other multinational corporations, including Microsoft and Cisco have been implicated in actions related to governmental censorship and use of electronic information in China, this paper will largely focus on these two cases. This is for two main reasons: 1) there is more concrete information present regarding the actions of Yahoo! and Google, and 2) for brevity's sake.

Case 1: Yahoo!, Alibaba, and Shi Tao

In 2007, two Chinese journalists sued Yahoo! for abetting torture. They said that because Yahoo! provided information to the Chinese government, the company aided the Chinese in the subsequent arrests and torture of Wang Xiaoxing and others.[9] This must be coupled with the arrest of Shi Tao.[10] In that case, Yahoo! Holdings, Ltd. (based in Hong Kong) provided the information to the Chinese government, stating, "Yahoo! must ensure that its local country sites must operate within the [local] laws, regulations, and customs."[11] The practices of Yahoo! go as far back as 2003, when Yahoo! was accused of helping the Chinese government get information on Li Zhi, an anticorruption reformer.[12] These issues stem from Yahoo!'s involvement with Alibaba.com, which is a Chinese company that is 40 percent owned by the Chinese government.[13] Yahoo! officials said in the aftermath of these issues that their company's close ties with Alibaba were an "important point to make."[14] The connection with Alibaba also suggests a distinct problem for those who believe that the United States should pass legislation to stop such actions from occurring. According to Jeffrey MacDonald, writing for the *Christian Science Monitor*, "For its part, Alibaba.com suggests Beijing policy would trump laws that Congress might pass."[15] Officials continue to talk about the importance of local laws and customs as the reasons why Yahoo! in China has given up so much information. However, it is also worth noting that Yahoo! is only a minority stakeholder which would make legislating their actions in China difficult.[16]

Case 2: The Google Case

Much more recently, Google and China became engaged in a disagreement over a series of cyber attacks that occurred against the Google computer network. Google claimed that

9 William A. Cohn, "Yahoo!'s China Defense," *The New Presence, 10*(2): 30.
10 Marqueland, "Yahoo!, Chinese Police, and a Jailed Journalist," 7.
11 Ibid.
12 MacDonald, "When Yahoo! in China is Not Yahoo!," 1-2.
13 Ibid.
14 Ibid.
15 Ibid.
16 Ibid.

these attacks, leveled at their organization and many others, served to attempt to infiltrate the e-mail accounts of numerous human rights activists in China. In early 2010, Google announced that it would reroute all its search engine capabilities on the general Google.cn site (China's version of Google.com) to Google.com.hk, based out of Hong Kong. This would allow for people who were behind the "Great Firewall of China" to be able to search freely on Google. Later in 2010, Google.cn was replaced with a page that only bore a link to Google.com.hk and was unable to be used to search. Surprisingly, considering the typical hard line stance taken by China regarding companies that rebuff their attempts to control the internet, Google had its Internet Cache Protocol (ICP) license renewed in China in July 2010.[17] These licenses are required in China to provide internet content. If Google's license had been revoked, they would have lost access to a potentially enormous market. This renewal may be important because of the impact of hackers in the Google case. When it is considered that the ICP license was never in question because of a refusal to comply on behalf of Google (other than a refusal to continue its Chinese site), it is less shocking the license was renewed. Once it was renewed, the method Google was using to conduct searches was the same as before: a landing page at www.google.cn, which led to a link for www.google.com.hk. This shows a distinction between cases such as Yahoo's (in which the company must comply with a government request) and Google's (in which a company is given some leeway in protecting its information from third parties). However, it is still an open question as to how stable the Google system in China is currently, since it would certainly be possible for China to block www.google.com.hk in the future. Also, search services on Google Hong Kong could encounter any of the many problems of searching on Google's main search engine, including a slow and unstable search procedure that limits the ability of the program. Many pointed out that Google was not a major player in the Chinese internet market; however, Google does serve as a major company in the international internet market, with a well recognized search engine, e-mail client, and numerous other applications.

Differences between the Cases

Since the 2005 merger of Alibaba and Yahoo!, there was little control of Yahoo!'s operations in China, and Yahoo! would have encountered numerous difficulties in trying to leave the country. In contrast, Google had a smaller market share and no major Chinese partner, which may have made it easier for that company to buck the Chinese government. However, they still attempted to first reroute their services before coming to a point where there services were largely removed from China. Thus, there are two major differences between these two cases. On the one hand, we have a company (Yahoo!) that is controlled by an agreement that was signed between the company and Alibaba. On the other, we see the reaction of a more independent company (Google). Since Alibaba is so tied to the Chinese government, Yahoo! would logically tilt toward acquiescing to requests from the Chinese government. This is compounded by the presence of a concrete governmental request. Google, which is not tied to the Chinese government, would not have such corporate impulses, especially considering the nature of the case (which involved third party attacks, not governmental requests).

17 "An Update on China: The Official Google Blog, July 6, 2010," accessed November 10, 2010, http://googleblog.blogspot.com/2010/06/update-on-china.html.

Hacking to gain information is not an uncommon practice in China. In recent history, programs like GhostNet have been implicated in the disappearances or arrests of Chinese human rights activists. Stories can be as extreme as programs that turn on webcams to be able to snap a picture of the alleged human rights activist sitting at his or her computer. While this is devious enough, it is compounded by the fact that these webcams are turned on, but the light on the computer that lets the user know the camera is on is commanded to remain unlit.[18] Thus, such hacking blends espionage and information gathering. GhostNet was responsible for the arrests of several Tibetan dissidents who were arrested as they re-entered China. GhostNet reached servers for the Netherlands-based and US-based International Campaign for Tibet (ICT), as well as numerous other organizations.[19]

It is a possibility that, because Google had such a low standing in the Chinese economy and was not partially owned by a Chinese giant like Alibaba, Google was selected to be attacked by a wave of hacking to gain information. In the cases of Yahoo! in recent memory, information was disclosed very easily from the company to the government, upon request. In the case of Google, there was an offensive strike that sought to take the requisite information. This could be due to the fact that Google initially refused the requests or lacked the physical presence in China for requests to be made. It is also possible that there are simply numerous nationalistic hackers in China, attempting to gain information regarding human rights activists. Such hackers in other countries (especially Russia) even have a name – "patriotic hackers" – and have engaged in extreme behaviors in an effort to ruin Estonia.[20] However, because of attribution problems arising from the diffuse nature of the internet, it is hard to tell if the Chinese hackers are members of the Chinese government or if they are merely citizens with computers and an ax to grind with the Western world.

Regardless of Google, Yahoo!, or Alibaba's clout within the Chinese market, economic concerns must be addressed when looking at this issue. The Chinese market is large, now boasting nearly 400 million users of the internet.[21] This is what Surya Deva calls the "China Factor," the lure of the large Chinese market, regardless of whether a company can break into that market or can act in an ethical manner once it has done so.[22] Deva notes that Yahoo!, which was an early player in the internet in China, arriving into the market in 1999, became immediately complicit in the country's internet censorship regime before moving on to providing private information regarding users.[23] Yahoo! has been called the worst offender regarding corporate complicity with internet censorship in China.[24] Many of these problems, particularly regarding the provision of private information by Yahoo! to the government, may stem from 2005, when Yahoo! merged with Alibaba. Deva argues that this allowed for Yahoo! to blame its subsidiary company for the actions it took in China. Yahoo!'s defense following

18 Information Warfare Monitor, "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor,* March 29, 2009.
19 Ibid.
20 James A. Lewis, "Cyber Attacks Explained," *CSIS Commentary,* June 15, 2007.
21 Chris Buckley, "China Internet Population Hits 384 Million," *Reuters*, January 15, 2010.
22 Surya Deva, "Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?" *George Washington International Law Review 39*(2007): 261.
23 Ibid., 267.
24 Ibid.

incidents such as Shi Tao has been to argue that Yahoo! does not have day to day control over their actions in China.[25] Another defense offered by Yahoo! executives regarding their actions in China was that, because such actions have been legally mandated by the Chinese government, Yahoo! was forced to comply or its staff in China could have been arrested. In short, as per Michael Callahan, the Senior Vice President of Yahoo!, "Ultimately, American companies face a choice: comply with Chinese laws or leave."[26] Here is where we see the pull of the large Chinese market, for, as Deva says, it would be highly unlikely that companies would choose to accept such blatant behavior in other countries like Myanmar or Zimbabwe.[27]

The Effects of the Current International Legal System

The bulk of international law on this subject comes from two sources: The Global Online Freedom Act and the Global Compact. The Global Online Freedom Act and the Global Compact have unfortunately come up short in stopping corporate complicity with regards to authoritarian states and the internet.[28] This is because companies have routinely flouted the regulations promoted by the UN's Global Compact and, in cases where they made agreements, were woefully lacking in implementation. Surya Deva argues that, while two of the principles of the Global Compact are directly related to the notions of internet freedom in China and the provision of private data to the Chinese government, Google and Yahoo! have not actually accepted the Global Compact as a defining part of their role in China.[29] However, it is also noted that the Global Compact serves as an offshoot of human rights norms posited by the United Nations, along with a string of UN rights documents, which make general demands of companies regarding their human rights record.[30] Deva further notes, though, that these mechanisms do not talk in detail about the actions those companies should take in situations where they are found by shareholders to be complicit in human rights abuses. Further, there is also the problem of subsidiary companies and parent companies, as is seen here, with the case involving Yahoo! and its Chinese subsidiary. This is especially pronounced in Yahoo!'s case, considering their lack of control over day to day operations, given that they gave said control to Alibaba.[31] Thus, it can be seen that enforcement of the Global Compact and, by extension, international human rights norms on corporations is quite difficult given the confusing landscape presented.

Perhaps the biggest problem with the Global Compact is that it is not a regulatory instrument. As per Deva, the regulations are, at best, "one liners" that provide little in the way of nuanced or detailed regulations.[32] Deva argues that this was largely to keep the deal attractive for corporations, who saw the compact as a way to dissuade anti-globalization forces around the world by giving the UN what it wanted regarding the Global Compact.[33] In short, the

25 Ibid., 267-68.
26 Ibid, 268.
27 Ibid., 261.
28 Ibid., 257.
29 Ibid., 279.
30 Ibid., 279-80.
31 Ibid., 281-83.
32 Surya Deva, "Global Compact: A Critique of the UN's "Public-Private" Partnership for Promoting Corporate Citizenship," *Syracuse Journal of International Law and Commerce, 34*(2006-2007): 129.
33 Ibid., 110, 129

Global Compact provides the norms and standards to companies who accept them. However, it provides no methods for enforcement when a company breaks those regulations.[34] As an instrument, it does not even measure good and bad behavior. The Compact simply leaves the enforcement and enlightenment of corporations to the corporations themselves.[35] In short, the Global Compact is simply too vague and too reliant on self-enforcement to be effective, given the market pull of a country like China.

In regards to the Global Online Freedom Act, a piece of legislation posed in the United States, the complexities of international law on this issue make enforcement difficult, even though the law shows promise in theoretically stopping such abuses.[36] Deva finds little evidence that the Global Online Freedom Act would even be enacted and sees extreme problems regarding its enforcement.[37] The Act was put forth by Representative Christopher Smith in 2006 and has subsequently been referred to a series of committees and subcommittees within the United States. It is important to recognize that lawmakers are specifically targeting China's actions with this piece of legislation. According to William J. Cannici Jr., "While GOFA acknowledges nine Internet-restricting countries," China is the major offender and the primary target of the Act."[38] The Act itself has yet to pass, though it has already been in the works for several years.[39] Deva argues that the Online Freedom Act could serve as an important component in the *enforcement* of laws relating to internet freedom in countries like China.[40] This is because, as opposed to the Global Compact, the Global Online Freedom Act is much more specific in its language. The act says that, if a US company engages in any one of a number of acts, including providing private information on users to a government of an "internet controlling" state, the company can be punished. Such punishments would include those of both civil and criminal nature.[41] It is important to note that there are still issues with this proposed piece of legislation. According to Nellie Viner:

Section 201 of the Act would prohibit Internet companies from storing personally identifiable information in Internet-restricting countries. This means that the Act would prohibit companies "from locating any hardware associated with their services within a country designated" as Internet-restricting. As a result of this location restriction, the number of countries in which a server could be located would be greatly decreased. Consequently, an Internet search would unearth a much smaller number of results than if the server were located within the country in which the search was initiated. This is because servers located abroad are slower and limited by state-level firewalls and filtering.[42]

34 Deva, "Corporate Complicity in Internet Censorship in China," 293.
35 Ibid.
36 Ibid., 257-58.
37 Ibid., 258.
38 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," *Seton Hall Legislative Journal 32*(2007-2008): 125.
39 Deva, "Corporate Complicity in Internet Censorship in China" 309.
40 Deva, "Corporate Complicity in Internet Censorship in China" 311.
41 Ibid., 312-314.
42 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?" *The Iowa Law Review 93*(2007-2008): 383

Viner argues that the law should merely be amended and passed and that it would effectively aid all parties in the discussion of Chinese internet censorship. However, Viner herself notes that the important aspect of Section 201 is the ability of this provision to limit state use of the internet to violate privacy.[43] As such, we can see that the Global Online Freedom Act is at odds with itself. In trying to stop both censorship and privacy violations involving the internet, it has text that puts these two objectives in stark contrast. Viner also notes that, if Section 201 remains, foreign companies, many of whom will care less about human rights (and, in all likelihood, privacy of their users) than the United States does, would be able to take greater control of the internet.[44] As such, Section 201 itself might have little effect on the issue of privacy, further compounding questions regarding the legitimacy of legislation in this instance. Cannici notes, however, that newer iterations of this legislation have included a "presidential waiver," where the president can allow any company based in the United States to operate within an internet restricting country.[45] Thus, even one is willing to accept the trade-off posed by the Global Online Freedom Act, newer forms of the law open a potential loophole that could make its privacy violation powers moot. Perhaps the greatest obstacle to the Global Online Freedom Act is a lack of political will, considering that this law has yet to pass. It seems highly unlikely that it will be passed in its current form, given the issues with Section 201 and the reforms and amendments consistently proposed. The failure to actually put a stable law on the table indicates a significant problem of the current legal regime in addressing such problems.

Our Legal Disconnect: Telecommunications Immunity and Internet Censorship

Further, regarding the current legal framework, there is a disconnect regarding the effect and role of domestic telecommunications laws in the United States, which gave telecommunications companies immunity in regards to their actions supporting the War on Terror through domestic wiretapping or spying. The law, the Foreign Intelligence Surveillance Act Amendments Act of 2008 (Section 201), as signed into law July 10, 2008:

> Prohibits any federal or civil action against any person (including an electronic communication service provider or a landlord or custodian) providing surveillance assistance to an IC element if the AG certifies that such assistance was: (1) provided pursuant to an order or directive under FISA; (2) in connection with an intelligence activity authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, and designed to detect or prevent a terrorist attack against the United States; (3) the subject of a written request from the AG or IC element head to the provider indicating that the activity was authorized by the President and determined to be lawful; or (4) not provided. Allows for the judicial review of such certifications. Limits certification disclosure for national security purposes. Prohibits state law preemption of the protections afforded assistance providers under this section. Requires semiannual reports from the AG to the intelligence and judiciary committees on the implementation of this title. Title III: Review of Previous Actions.[46]

43 Ibid., 384.
44 Viner, "The Global Online Freedom Act" 385.
45 Cannici, Jr., "The Global Online Freedom Act," 139.
46 FISA Amendments Act of 2008, *US Code*, Title 110, Section 201.

This makes developing laws that punish companies engaging in such actions in foreign countries seem hypocritical, undermining their legitimacy. In an interview with Dr. Erick Novotny conducted on October 1, 2010, it was mentioned that the presence of such laws could serve as a lightning rod for those who would claim that the United States is being "imperialistic" or "hypocritical" as a country by demanding China stop its efforts to gain confidential information.[47] He mentioned that Justice Department officials, when they attempted to investigate the actions of the Pentagon regarding domestic wiretapping, had their security clearances revoked. The overall message, according to Novotny, was that security trumped criminal activity.[48]

Novotny also discussed the company Narus, which is a California company with offices in Shanghai. Narus is staffed by former NSA officers, and one of its main jobs is to make tracking software that can specifically locate dissidents. Its goal in these situations is to create complete network and data visibility.[49] These domestic issues are a huge blow to the ability of the U.S. government to conduct diplomatic actions with the Chinese on this issue. This is specifically true given the fact that former NSA staffers are operating a company that is doing exactly what the United States would be lobbying against. The presence of Narus is more than corporate complicity; it is indeed corporate action to suppress human rights. Thus, while it might on face seem like a good time for the Obama Administration to be making a lot of noise regarding human rights with China, these issues have largely been traded for bigger, macroeconomic concerns.[50] There is a definite possibility that this has occurred because the United States feels it has "lost the high ground" on this issue, given the presence of both the telecommunications immunity presented in the FISA Amendments Act and the presence of companies like Narus. Combining this with China's improved economic stature, there is a definite possibility of a situation in which the United States does not have the leverage to be able to limit China on this issue.[51]

Alternative Solutions

There are severe drawbacks to the proposed solutions to these problems. In place of these solutions and the current policy, this paper will recommend a mixed approach as a possible alternative. In the end, it will be conceded that, within a shifting and confusing domestic and international political spectrum, a coherent strategy will be hard to come by. Thus, there must be action on the part of both governmental and non-governmental actors in fixing such problems. The current legal regime that has been put forward is ineffective. Future solutions have been complicated by other actions taken by the United States government, specifically United States laws that grant immunity to telecommunications companies. There is a need for stringent lobbying of the United States government, the Chinese government, and the companies themselves, on behalf of both trade unions and non-governmental human rights organizations. Efforts in the United States should be to form a coherent and easy to navigate legal regime on the issue of internet privacy. Lobbying efforts against the Chinese and the

47 Eric Novotny, Interview with author, Washington, DC, October 1, 2010.
48 Ibid.
49 Ibid.
50 Ibid.
51 Ibid.

companies should be to name, blame, and shame them into reforming their practices on the subject.

Aside from the options previously discussed with regard to legal frameworks to address this issue, either coming from the United States or internationally, there are several alternative policy options to consider. Here, I will examine four: (1) use of the Foreign Corrupt Practices Act, (2) development of policies by individual business groups, (3) promotion of a "naming, blaming, and shaming" effort, both by the United States and the international community, and (4) strengthening of US diplomacy efforts.

Use of the Foreign Corrupt Practices Act (FCPA)

The FCPA was enacted in 1977 to prevent actions of bribery on the part of US companies operating abroad. The act makes it illegal for a company to provide anything of value to a government official to get preferential treatment.[52] The question becomes whether or not the provision of information to government officials, as occurred with Yahoo! and other companies, serves as the provision of something valuable. Certainly, the Chinese government would find such information valuable, as it values preventing dissidents from disturbing the rule of the current regime. However, how is something of value defined within the law? Unfortunately, there is no specific definition laid out for an item of value, under this regulation. Further, even if we were to take a liberal view of the definition of something of value to include private information, as per the Department of Justice, we must still show that the information was given with "corrupt intent" or the intent to have a foreign official ignore his professional duties in order to funnel more business to the company in question.[53] None of the actions of Yahoo! or any of the other companies in question would indicate they have done any more than merely work within the framework of the Chinese system to maintain business there, and thus their efforts have not been to funnel more business to them. In the case of Google, which did not have a large market share in China, this is especially noteworthy. These actions seem to actually conform to the jobs of the various foreign officials, making the Foreign Corrupt Practices Act untenable in this situation.

Viner notes that the Global Online Freedom Act is "analogous" to the FCPA in that it gives jurisdiction to the Department of Justice and is extremely clear regarding these issues.[54] However, while she notes that the FCPA has been the hallmark of legislation similar to the Global Online Freedom Act since its inception, she makes no attempt to argue for its use in battling these problems. Rather, she uses the presence of the FCPA to argue for the passage of the Global Online Freedom Act. This pending piece of legislation has its own issues, which we have already investigated, but Viner's discussion shows that the FCPA has problems of its own. Namely, it is too focused on bribery and corruption to be re-tasked to focus on internet censorship and privacy violations. Further, if the Global Online Freedom Act is the new leg-

52 The Foreign Corrupt Practices Act of 1977, 15 U.S.C. §§ 78dd-2.

53 "The Foreign Corrupt Practices Act, Anti-Bribery Provisions: Lay Persons Guide," *The United States Department of Justice Fraud Section,* accessed November 10, 2010, http://www.justice.gov/criminal/fraud/fcpa/docs/lay-persons-guide.pdf.

54 Viner, "The Global Online Freedom Act" 390.

islation that does just that, examination of the Global Online Freedom Act shows that such a re-tasking is inefficient at best, and, at worst, actually damaging to privacy, given Viner's concerns about Section 201.[39]

Corporate Codes of Conduct and Policies Developed by Business Groups

Often, problems such as these have to be regulated by internal controls. Companies and their respective trade associations must come together and develop policies for such issues. A classic example of this regarding the internet is Google. Google states that one of its core principles is that the company can "make money without doing evil" and that "the need for information crosses all borders."[55] Further, one could argue that the Global Compact, as described above, is a form of trade association language, articulating a series of general principles regarding business practices and human rights. However, such general statements have clearly failed as a method for ensuring that companies do not engage in corporate complicity regarding human rights abuses. Thus, what is needed is a more specific form of trade association policy or corporate code of conduct. However, such a code of conduct or policy is difficult to devise. Novotny explains that this is because trade associations and business groups must conform to the lowest common denominator to please all of their members. Thus, truly controversial issues such as this one or the issue of net neutrality receive little in the way of concrete, specific regulations because the members have difficulty in agreeing to terms on the subject. The major problem in this situation is that each of these companies is playing an active and different role within this system and, thus, each has different viewpoints.[56] This inherent confusion makes the use of trade association or corporate policies alone meaningless. Thus, we must try to add other measures to this discussion, involving governments and non-governmental sources.

Naming, Blaming, and Shaming

The idea of naming, blaming, and shaming has existed in the human rights discourse for quite some time. The idea, according to Emile M. Hafner-Burton, is to take a country, call it out for its actions, and blame it for its actions, with the hope of shaming it into stopping the action in question.[57] However, if such tactics have been used against countries, could they not also be used against corporations that engage in actions found to be in violation (or complicit in the violation) of human rights? Hafner-Burton makes the point that, largely, these tactics are effective in bringing about things like elections or political protections, noting that these tactics seem to have the most trouble in stopping governments from terrorizing their citizenry.[58] Such actions could easily be combined with boycotts and other measures that affect the bottom line of these companies. As Novotny puts it, only about one percent of the base for Google or for Yahoo! exists in China. Thus, there seems to be little reason for

55 "Our Philosophy, No. 6 and No. 8," last updated September 2009, accessed November 10, 2010, http://www.google.com/intl/en/corporate/tenthings.html.
56 Novotny, Interview.
57 Emile M. Hafner-Burton, "Sticks and Stones: Naming and Shaming the Human Rights Enforcement Problem," *International Organization, 62*(4): 689.
58 Ibid., 691-92.

these companies to make such a moral compromise for this limited share.[59] However, he also notes that many of these companies may pursue such issues regardless of the moral questions involved because it is difficult to present a logical economic argument as to why you refuse to enter into a country that has one fifth of the world's population, simply because the process is "hard."[60] Thus, again, we can see the pull of the market in China. For naming, blaming, and shaming tactics to work effectively, they would likely have to be aimed at three targets. The first is the company in question. The second would have to be the Chinese government, and the third would have to be the United States government. This third element would be implemented to combat the policy paradoxes presented by the United States, which could provide cover for the companies or the Chinese government going forward.[37]

A major problem with the use of naming, blaming, and shaming techniques may be one of politics. As Hafner-Burton puts it:

Whether and how naming and shaming works might also depend on when and where the spotlight is shone. Organizations—whether NGOs, news media, or the UN—shine the spotlight selectively. Some countries guilty of horrible abuses never draw much publicity, while others responsible for lesser abuses draw much attention. For instance, political terror has been widespread in Uganda and North Korea for decades, yet these countries receive far less publicity from the international community than do Cuba, China, South Africa, or Turkey, which are more often put in the spotlight for less severe abuses.[61]

Considering that China has had a history of claiming Western Imperialism, such a double standard could be extremely detrimental to the effectiveness of these tactics. However, if organizations and others are careful to aim their tactics squarely at the companies and make sure that they also address the issues cited above that pertain to the United States, these tactics might be somewhat effective. In the end, Hafner-Burton is probably right in declaring such actions to not be simply "cheap talk" but not a cure-all either.[62] To truly make these actions effective, they should be combined with strong diplomacy from the United States and a newfound push for stronger and more specific trade association policies, which could come as a result of these campaigns.

Stronger US Diplomacy

Perhaps one of the most effective measures that could be taken would be a stronger position by the United States government regarding these issues. With a major international hegemon like the United States pushing on the Chinese to stop these actions, more headway could be made. However, as Novotny states, the major problem is that the U.S. Department of State has been incredibly uneven on this topic. It appears for brief moments, such as in statements made by Secretary of State Hillary Clinton in January 2010, but then it fades away. Clinton said in January 2010:

59 Novotny, Interview.
60 Ibid.
61 Hafner-Burton, "Sticks and Stones," 694.
62 Ibid., 707.

On their own, new technologies do not take sides in the struggle for freedom and progress, but the United States does. We stand for a single internet where all of humanity has equal access to knowledge and ideas. And we recognize that the world's information infrastructure will become what we and others make of it. Now, this challenge may be new, but our responsibility to help ensure the free exchange of ideas goes back to the birth of our republic. The words of the First Amendment to our Constitution are carved in 50 tons of Tennessee marble on the front of this building. And every generation of Americans has worked to protect the values etched in that stone.[63]

Novotny notes that this problem with the U.S. position may be compounded by two facts. First, the United States has weakened its position regarding its telecommunications immunity laws and the presence of companies like Narus, which engage in actions that may actively violate the privacy of dissidents. Second, the United States may have finally recognized that China has become too powerful economically and that our economic clout no longer carries the requisite leverage for this kind of heavy handed diplomacy.[64] Also, Novotny points out that the reason we reopened our relations with China was to try and use free market tactics to liberalize their system.[65] It would seem unlikely, then, for the government to attempt to strong arm the Chinese on this issue, instead falling back on capitalist adages about the invisible hand of the market leading to greater freedom. However, at the very least, a consistent position by the State Department should be taken on this subject in order to allow for other measures—including naming, blaming, and shaming—to have an impact.

Policy Recommendation

In order to solve the problems put forth by the Chinese regime's attempts at internet censorship and the use of the internet to gain private information about dissidents, something more than a single-pronged approach is necessary. Mere legislation or corporate policies will not be enough to stop such a problem. The reason for this is simple. There are too many players and too many variables within this system. Without a multi-pronged approach in which actions are taken to give one solid outcome—specific and enforceable laws and policies on the subject—the system becomes increasingly confusing and unenforceable. This can be seen from the failure of the Global Compact and the inability of the Global Online Freedom Act to be passed. As long as there is no unified response from the United States government and no unified campaign from the media, NGOs, and others, we can expect little change on this subject.

Thus, this author recommends the following actions:

A vigorous naming, blaming, and shaming campaign should be conducted. The major targets should be (in order): the individual companies, the Chinese government, and the United States government. This campaign should target the actions of the companies and the policies of the Chinese government, while admonishing the United States for its recent

63 Hillary Clinton, "Remarks on Internet Freedom," *United States Department of State*, January 21, 2010, accessed November 27, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm.
64 Novotny, Interview.
65 Ibid.

telecommunications immunity bills, which have only served to muddy the waters on this issue. This campaign should be supplemented by boycotts and other measures that could have effective economic impacts on the companies in question and their various advertisers. Any actions taken against the United States government should call for the immediate repeal of the telecommunications immunity laws so that the United States can put more forceful and meaningful pressure on authoritarian governments, such as the Chinese. In place of such laws, legislation like the Global Online Freedom Act would be beneficial. However, without removing immunity provisions, these laws would do little but provide a confusing and uneven international legal landscape.

The US government should adopt a uniform policy for addressing the Chinese government on these issues. The US government must choose whether or not to focus on the macroeconomic issues within their relationship with China or the human rights issues. Human rights issues can no longer vanish from the discussion only to reappear again later. Further, this paper would strongly urge the repeal or, at the very least, rewording of the telecommunications immunity laws that were put into place during the War on Terror. These laws do little more than confuse this issue and give the Chinese government and the various companies involved a place to hide, arguing that the United States government is engaging in activities that are hypocritical by having such laws on the books. Passage of legislation similar to the Global Online Freedom Act would also be helpful, but not without first removing the telecommunications immunity legislation currently on the books.

Based off of these two actions, trade associations and companies must come together and attempt to develop coherent, enforceable, and specific codes of conduct that discuss issues of censorship and privacy regarding the internet, their customers, and foreign governments. It would be especially important to include a discussion of how a company handles working with a third party within a foreign country (such as in the Yahoo! case) and how it handles laws that go against the general spirit of their corporate principles (as in the Google case). Further, these codes could help untangle situations in which third parties, such as hackers, violate privacy in ways unknown or unintentionally allowed by the company in question. Certainly, such situations are not as grave as situations in which a company hands information over to an authoritarian government. However, these situations should be mentioned, particularly in discussing methods to investigate such actions. Through investigation, culpability could potentially be placed. This could occur either for negligent officials and cyber criminals or for government officials shown to be sanctioning such actions.

Conclusion

This paper argues that a three-pronged approach, while not a perfect solution to this problem (there is truly little that can be done if China still wants to invade the privacy of its citizens) is the best solution to this problem, given the circumstances. That is to say that this multi-pronged approach is certainly better than the current single-pronged approach. This is because, by adding in a unified campaign of naming, blaming, and shaming, the international community might be able to force one party within this issue to alter their policies on this matter. Most likely, the companies themselves would be forced to alter policies because of the

possibility of tangible, economic losses that could be suffered due to the boycotts and other measures that should be combined with the naming, blaming, and shaming efforts. However, in order to work effectively, this campaign will need to be bolstered by no less than a unified response from the US government. The issue of human rights in the US-China relationship cannot keep disappearing and reappearing. The telecommunications immunity laws that have been passed by the United States are an Achilles Heel to this issue, forcing the United States to push forward and back pedal on this issue at all times. Removing this possibility by passing more stringent legislation would enable the United States to force the Chinese to be more mindful of international norms regarding privacy.

References

Buckley, Chris. "China Internet Population Hits 384 Million." *Reuters*. January 15, 2010.

Cannici, William 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." *Seton Hall Legislative Journal 32*(2007-08): 123-166.

Clinton, Hillary. "Remarks on Internet Freedom." *United States Department of State*. Last updated January 21, 2010. Accessed November 27, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm.

Cohn, William. "Yahoo!'s China Defense." *The New Presence 10*(2): 30-33.

Deva, Surya. "Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?" *George Washington International Law Review* vol. 39. 2007. 255-319.

---. "Global Compact: A Critique of the UN's "Public-Private" Partnership for Promoting Corporate Citizenship." *Syracuse Journal of International Law and Commerce 34*(2006-2007): 107-151.

FISA Amendments Act of 2008. *US Code*. Title 110. Section 201.

Foreign Corrupt Practices Act of 1977. 15 U.S.C. §§ 78dd-2.

Google. "A New Approach to China: The Official Google Blog, January 20, 2010." Accessed May 31, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

---. "A New Approach to China: The Official Google Blog, March 22, 2010." Accessed May 31, 2010, http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html.

---. "An Update on China: The Official Google Blog, July 9, 2010." Accessed November 10, 2010, http://googleblog.blogspot.com/2010/06/update-on-china.html.

---. "Google China." Accessed November 10, 2010: http://www.google.cn.

---. "Google Corporate Information: Our Philosophy, No. 6 and No. 8." Last updated September 2009. Accessed November 10, 2010, http://www.google.com/intl/en/corporate/tenthings.html.

Hafner-Burton, Emile. "Sticks and Stones: Naming and Shaming the Human Rights Enforcement Problem." *International Organization 62*(4): 689-716.

Human Rights Watch "Race to the Bottom: Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch 18*(8).

Information Warfare Monitor. "Tracking GhostNet: Investigating a Cyber Espionage Network." *Information Warfare Monitor.* March 29, 2009.

Lewis, James. "Cyber Attacks Explained." *CSIS Commentary*. June 15, 2007.

MacDonald, Jeffrey. "When Yahoo! in China is Not Yahoo!" *Christian Science Monitor 98*(55).

Marqueland, Robert. "Yahoo!, Chinese Police, and a Jailed Journalist," *Christian Science Monitor 97*(201).

Novotny, Eric. Interview with author. Washington, DC. October 1, 2010.

United States Department of Justice. "The Foreign Corrupt Practices Act, Anti-bribery Provisions: Lay Persons Guide." *The United States Department of Justice Fraud Section.* Accessed November 2010. http://www.justice.gov/criminal/fraud/fcpa/docs/lay-persons-guide.pdf.

Viner, Nellie. "The Global Online Freedom Act: Can U.S. Internet Companies Scale the Great Chinese Firewall at the Gates of the Chinese Century?" *The Iowa Law Review 93*(2007-2008): 361-392.

Watts, Jonathan. "How Internet Giant Google Turned on Gatekeepers of China's Great Firewall." *The Guardian*. January 14, 2010.

"Yahoo!'s Defense in Case of Jailed Dissident." *Business Week Online*. November 7, 2007.