Postscript on China

Dorothy E. Denning
9 June 2006

My earlier article mentioned that hackers had targeted Chinese government computers in the name of democracy and human rights. China's border routers were configured to block access to certain websites outside the country, and the hackers had disabled the blocking in some of the routers, thereby allowing access to otherwise forbidden websites.

The objective of this postscript is to briefly review some of the events that have transpired since I wrote my article regarding Internet censorship in China. These range from the development of tools to circumvent the firewalls to expressions of outrage over the practices of U.S.-based corporations doing business in China. I will discuss the issues raised by these activities and the challenges they present.

Circumventing the Firewalls

Hackers and software developers in the United States have developed various software tools that allow Chinese users to access information blocked by the firewalls. The tools make use of such technology as proxy servers and networks, encryption, steganography, peer-to-peer file sharing, and tunneling protocols. Examples include Anonymizer and Tor technology, Dynamic Internet Technology's Freegate and DynaWeb, Safe Web's Triangle Boy, UltraReach's Global Internet Freedom Technology, Peacefire's Circumventor, The University of Toronto Citizen Lab's Psiphon, and Hacktivismo's Six/Four and Camera Shy. The U.S. government, through the Broadcasting Board of Governors (BBG), has funded some of these efforts in order to ensure access to its Voice of America and Radio Free Asia websites.[1]

Anonymizer Inc., which is mentioned in my earlier article for its Kosovo Privacy Project, was one of the first companies to offer proxy web services to facilitate anonymous browsing and access to information. In spring 2006, they launched Operation Anti-Censorship to help Chinese users access blocked sites. A similar service has been available to users in other countries, including Iran. With the Chinese service, users are given the URL for a website outside China where they can register and download special software. To avoid being blocked itself, the URL for the Anonymizer site is constantly changed and users notified via e-mail.[2]

Six-four and Camera Shy were developed by Hacktivismo, a group of hackers, human rights workers, lawyers, and artists. Six-four uses peer-to-peer file sharing with encryption and tunneling to get documents past government filters, while Camera Shy uses steganographic techiniques to hide information inside a cover medium such as an image file.

Hacktivismo evolved from the Cult of the Dead Cow (cDc), a group mentioned in my earlier paper for denouncing proposed cyber attacks to disable the networks of China and Iran as contrary to improving these nations' free access to information. cDc's foreign minister, Oxblood Ruffin, founded Hacktivismo and has been outspoken on the need for cyber activists to support rather than hinder human rights efforts. He condemned web sit-ins organized by the Electrohippies, calling them denial of service attacks in violation of the freedoms of expression and assembly. He said that "One does not make a better point in a public forum by shouting down one's opponent."[3] The Electrohippies justified their sit-ins on the grounds that they provide a focus for debate about the organizations they target and "substitute the deficit of speech by one group by encouraging debate with others."[4]

Complying with Censorship

While some U.S. companies have been praised for the efforts to promote information flows into China and other countries that censor the Internet, others have been chastised for supporting the censors, even if only indirectly. Among the latter are four big industry names: Cisco, Microsoft, Yahoo!, and Google.

Cisco has been criticized for supplying routers to China with a firewall function that can be configured to block certain IP addresses. Because Cisco has no control over how its routers are configured and firewalls are used, the only way they could prevent their routers from being used to censor would be to remove the firewall feature. However, the blocking capability is needed to defend against Internet attacks, including denial-of-service attacks and IP spoofing attacks. If Cisco were to remove this feature from their Chinese routers, they would be doing a great disservice to their Chinese customers and the victims of Internet attacks.

While Microsoft has also been criticized for supplying software to aid the censors, the biggest objections arose when it removed the blog of a prominent Chinese blogger, Zhao Jing, at the request of the Chinese government. Critics were especially outraged at the closure given that the blogging site on MSN Spaces was hosted outside China. Following the incident, Microsoft expressed regret for closing the site and announced a policy for dealing with future incidents. That policy has three aspects. First, Microsoft will remove access to blog content at the request of a government only if it receives a legally binding notice from the government that the material violates local laws. Second, it will remove access only in the country issuing the order, allowing continued access outside that country. And third, it will notify users that the material was blocked due to government restriction. Microsoft also argued that MSN Spaces, which had attracted more than 3.5 million users and 15 million readers since its introduction in China in May 2005, was a powerful tool for economic development and freedom of expression.[5] Jing himself agreed that, while he was unhappy with the decision to close his blog, on balance, Microsoft was helping people speak publicly. Jing also admitted that he had crossed the line in one of his postings by calling for a boycott against a newspaper for firing an editor. He said that whereas the government was fairly tolerant of speech, they cracked down on activities seen as organizing political action.[6]

Even more ire was directed at Yahoo! for providing information about one of its account holders to Chinese authorities in 2004. That information led to the arrest and conviction of a Chinese journalist, Shi Tao, who was sentenced to ten years in prison for using his Yahoo! China account to leak details of a government document on press restrictions to a pro-democracy website run by Chinese exiles in New York.[7] Yahoo! justified their actions on the grounds that Yahoo! China operates within China and is under legal obligation to adhere to China's laws, and that failure to comply could subject Yahoo! China employees to criminal charges, including imprisonment. Yahoo! also reported that when they supplied information about Tao, they did not know the nature of the investigation, which is typical of similar situations involving law enforcement demands for records in the United States and other countries. Since October 2005, Yahoo! China has been owned by a Chinese company, Alibaba.com, removing control from the U.S.-based company.[8]

When Google first started providing services in China, users visited a Chinese-language version of Google.com that was hosted on a server outside China. Google provided no filtering, but the search results passed through China's firewall before reaching the user. One consequence was that users would see sites listed in the search results that they could not access. Over time, Google also learned of other problems. Access to its website was slow, in some cases producing results that stalled out the user's browser. Some services, including Google News and Blogspot, were unavailable most of the time. Even Google.com was sometimes blocked. As a result, Google was losing out to Chinese competitors with inferior services.

After reviewing the situation, Google decided to open an office in Beijing and host an additional search engine within China at Google.cn. In doing so, it needed to comply with China's regulatory environment, which meant filtering out material categorized as illegal by the government. All ISPs in China are required to adhere to China's regulations and operate censorship mechanisms, although implementation is left to them. Google said they would continue providing the unfiltered, Chinese-language interface on Google.com; that they would provide users with a clear notification when links were removed from search results; and that they would not provide their other services such as Gmail and Blogger until they were confident they could protect the privacy and security of users' information.[9]

The introduction of Google.cn raised objections similar to those against the other companies. Many asked how a company with the motto "Don't be evil" could participate in censorship. Google's response has been to express a commitment to satisfying the interests of users; expanding access to information to people who want it makes the world a better, more informed, and freer place; and responding to local conditions. They believe the Internet is transforming China to the better, and that their services are making a positive contribution.[10] Even Zhao Jing, the blogger shut down by Microsoft, said he thought that Google was genuinely improving the quality of information in China and trying to do its best within a bad system.[11]

Conclusions and Suggestions

U.S. corporations doing business in China have little choice but to follow China's laws and regulations. It is either put up or pull out. No company can defy the laws of a country when operating within its borders without risking criminal prosecution of its employees and eviction. Businesses have little negotiating power, as other companies, both within and outside China, will gladly fill any vacuum. Moreover, U.S. companies can make a reasonable argument that their products overall promote the flow of information in China. They are trying their best in a difficult situation, adopting policies that protect speech and privacy to the extent possible within China's laws.

Some U.S. companies have expressed support for the adoption of industry guidelines for businesses operating in countries that restrict access to information. Google suggests that guidelines might encompass principles regarding disclosure of practices to users, protections for user data, and periodic reporting about governmental restrictions and the measures taken in response.[12] By adopting common practices, companies might better support the free speech and privacy rights of Chinese citizens, and be less vulnerable to bad decisions and criticism.

Some companies have also asked for greater support from the U.S. government in promoting the free flow of information. Google urged the government "to take a leadership role on government-to-government basis."[13] Yahoo! asked that the U.S. Departments of State and Commerce and the office of the U.S. Trade Representative "continue to make censorship a central element of our bilateral and multilateral agendas." Although the U.S. government may have greater leverage dealing with China than U.S. companies, it is hard to see the U.S. government convincing China to relax its censorship, especially considering recent events leading to allegations of human rights abuses by the U.S. government (e.g., Abu Ghraib and Guantanimo).

The U.S.-China Economic and Security Review Commission recommended increased funding for the BBG's Internet anti-censorship activities and the creation of "an entity within the executive branch to develop a comprehensive strategy to combat state-sponsored blocking of the Internet and persecution or harassment of users."[14] There is also a bill before the U.S. Congress, The Global Internet Freedom Act (H.R. 2216) to establish an Office of Global Internet Freedom within the International Broadcasting Bureau, which is overseen by the BBG. The new office would develop and implement strategies to combat state-sponsored Internet jamming and the intimidation and persecution by those governments of their on-line citizens."

In considering overall policy, it is important to take into account the collective efforts of all involved. While Google may be forced to block access to certain websites, the information may still get through via an anti-censorship product. The net result is an environment that brings considerable information into China. A worst case scenario would be for China to cut itself off from the Internet, becoming more like North Korea or Cuba. This is unlikely to happen given China's recognition of the value of the Internet to its economy, but the presence of U.S. companies in China's market likely fosters better

information flows and better relations between the U.S. and China. Over time, as the youth of China who have grown up chatting and blogging on the Internet assume positions of authority, China may adopt a more permissive information policy.

Endnotes

[1] Thomas Lum, Internet Development and Information Control in the People's Republic of China, CRS Report to Congress, RL33167, Congressional Research Service, Updated February 10, 2006.

[2] John Leyden, "Anonymizer Looks for Gaps in Great Firewall of China," *The Register*, April 3, 2006.

[3] Will Knight, "Hackers Question Denial of Service as Political Protest," *ZDNet*, March 13, 2000.

[4] Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act, Occasional Paper No. 1, The Electrohippies Collective, February 2000.

[5] Jack Krumholtz, Testimony before House of Representatives Committee on International Relations, Joint Hearing of the Subcommittee on Global Human Rights, Africa and International Operations and the Subcommittee on Asia and the Pacific, The Internet in China- A Tool of Freedom or Suppression? February 15, 2006.

[6] Clive Thompson, "Google's China Problem (and China's Google Problem)," *The New York Times*, April 23, 2006.

[7] Clive Thomson, "Google's China Problem (and China's Google Problem)."

[8] Michael Callahan, Testimony before House of Representatives Committee on International Relations, Joint Hearing of the Subcommittee on Global Human Rights, Africa and International Operations and the Subcommittee on Asia and the Pacific, The Internet in China- A Tool of Freedom or Suppression? February 15, 2006.

[9] Elliot Schrage, Testimony before House of Representatives Committee on International Relations, Joint Hearing of the Subcommittee on Global Human Rights, Africa and International Operations and the Subcommittee on Asia and the Pacific, The Internet in China- A Tool of Freedom or Suppression? February 15, 2006.

[10] Elliot Schrage, Testimony before House of Representatives Committee on International Relations.

[11] Clive Thomson, "Google's China Problem (and China's Google Problem)."

[12] Elliot Schrage, Testimony before House of Representatives Committee on International Relations.

[13] Elliot Schrage, Testimony before House of Representatives Committee on International Relations.

[14] Carolyn Bartholomew, Statement before the Congressional Human Rights Caucus Hearing on Human Rights and the Internet – the People's Republic of China, February 1, 2006.