

Sources: Benjamin Weiser, "Doubting Case, A Prosecutor Helped the Defense," *N.Y. Times*, June 23, 2008, http://www.nytimes.com/2008/06/23/nyregion/23da.html?_r=1&pagewanted=all; Benjamin Weiser, "Settlement for Man Wrongly Convicted in Palladium Killing," *N.Y. Times*, March 31, 2009, at A19; Stone Phillips and Dan Slepian, "Murder at the Palladium," *Dateline NBC*, Sept. 8, 2008, available at <http://www.msnbc.msn.com>

[/id/6913736/ns/dateline_nbc-crime_reports//](http://id/6913736/ns/dateline_nbc-crime_reports//); Letter from Daniel Bibb to Alan Friedberg, Nov. 7, 2008; *Berger v. United States*, 295 U.S. 78, 88 (1935); Bruce A. Green, "Why Should Prosecutors Seek Justice?," *Fordham Urban Law Journal* 26 (1999); Plato, *The Apology of Socrates*, in Plato I: *Euthyphro, Apology, Crito, Phaedo, Phaedrus* (H. N. Fowler trans. 1914).

Google and the Cyber Infiltration

Xiaorong Li

In mid-January of this year, Google threatened to pull its business out of China unless China lifted filters of its search engine results that resulted in censorship of so-called "sensitive content." At the end of March, having obtained no concession from the Chinese government to back down on its draconian online censorship, Google acted on its threat by closing down its www.google.cn search engine, but diverting all searches on that page to www.google.hk, so that Mainland Chinese doing a Google search could continue to get results in the Chinese language. (Though google.hk is not filtered, all web contents found by Mainland Chinese users are universally filtered for "sensitive" materials.) The motives behind Google's decision are likely complex. But whatever its motives, Google may have done some good by spotlighting and picking a fight with cyber censorship and cyber infiltration. Google and other foreign Internet technology corporations should have protested a long time ago, even at the cost to their own profit, and should never have accepted censorship as a precondition for entering the Chinese market.

Many Americans may not know that Google's search engine in China, www.google.cn, very likely had accepted ethically compromising conditions set by Chinese authorities to filter "sensitive" words, thus contributing to upholding the Chinese government's Great Fire Wall to block Chinese users' access to open information online. An easy test could be performed to demonstrate how much information had been censored by google.cn. A user outside the Great Fire Wall could search for words such as "Tiananmen incident," or "Falun Gong," on both google.cn and google.com.

One would see two very different pages of search results. In volume, the google.com search produces 10-15 times more results than google.cn does. In content, predictably, the results out of google.cn are one-sided, reflecting the government's point of view. It is difficult for Chinese users to link directly to google.com and gmail (which is hosted outside China); connecting from China is either very slow or not accessible. And like all websites outside the country, once opened in China, google.com's search results are subjected to censorship—politically sensitive contents would also be filtered and some pages are blocked.

Engaging in self-censorship by filtering information that the Chinese government wants to block from users in China is a seriously questionable practice. Google has projected an *ethical* image of doing business about itself. Google wants to be known for its commitment to promoting online free communication and open information. Its corporate motto is "Do no harm." Any such ethical commitment comes with strings attached—that it should not be set aside for purposes of convenience or other (ethically irrelevant) gains such as market strategies. The generality and consistency requirements of ethical commitments mean that Google should never have entered China by accepting censorship as a precondition.

One plausible argument for entering the Chinese market even if it means obeying ethically compromising local regulations is this: Internet companies will get a significant market share of the world's largest pool of potential users, 1.3 billion. This will not only enable American companies to make a profit, but also

enable Chinese users to benefit from information technology. While some politically sensitive information is blocked, according to this argument, the vast majority of the Chinese population only need “un-sensitive” information about products, services, or daily life necessities in an increasingly modernized society.

This argument glosses over a morally problematic presupposition that the Chinese people, ruled by a different kind of regime, do not care about having the option of accessing free, undistorted information in an unobstructed cyber space. It is possible that this option, while available to all Americans, is not necessarily taken advantage of by everybody. It would be interesting to know what percentage of Americans regularly search online for information allowing them meaningful participation in democratic governance or supervision of the official exercise of power. It is fair to point out that the fact that voter turnout was not great in the last few presidential elections does not justify the conclusion that Americans do not care about having the opportunity of electing their president. Indeed, if surveys had shown that the level to which ordinary folks cherished open access of free information in China was much lower than the level found in the US, one would still not be able to draw conclusions about people’s informed preferences in the respective countries. The two populations would not have had the same experiences with free access to information or the same exposure to public debates about the ups and downs of government censorship.

Another complication factor is the reality that, after years of trying, most foreign Internet companies that entered China have not been able to claim significant shares of the Chinese market. Google has about a 30 percent share of the market, while its Chinese competitor Baidu takes more than 60 percent. Chinese companies are good at imitating foreign products, but also have fewer or no prohibitions against providing services—such as free music downloads—at the expense of certain regulations on copyrights and so on. And these companies are good at meeting the social and psychological needs of Chinese consumers. Google is the only one so far who has gone public about its frustrations and is willing to cut its losses, which may turn out to be insignificant in comparison to Google’s global revenues. Google may have calculated that the benefit of keeping its share of the Chinese market is not worth the cost of its intellectual property being hacked and the undermining of its global reputation.

Google made a fuss most likely because it is alarmed by the sophisticated, large-scale cyber attacks on its site and the sites of more than 30 other Internet companies doing business in China, intended perhaps to steal intellectual property or install spyware. Google must have had enough. The hacking of gmail accounts and stealing of intellectual property are only parts of the

Chinese government’s cyber war, combined with technical and non-technological tactics, for control of freedom of information on the Internet. These tactics have also been used to strike a sense of fear among China’s growing population of Internet users, whose number has reached 400 million. For example, in June 2009, government-controlled media accused Google of spreading unhealthy pornographic contents. Chinese cyber activists conducted an analysis of search words entered in the Google.cn search engine and found repeated searches from locations in Beijing for pornographic words. The frequency of such searches was later used by official media in their accusations against Google. Analysts believe that such deliberate acts are those of government-paid cyber thugs, known as “the

Google may have calculated that the benefit of keeping its share of the Chinese market is not worth the cost of its intellectual property being hacked and the undermining of its global reputation.

50 cents party” for the fee (in Chinese currency) they are paid for each posting favorable to the government’s position. The objective of the members of the “50 cents party” is to harass and inform on online activists, monitor contents of websites, blogs, and Twitter, infiltrate activists’ interactive sites or chat groups, and hack websites’ email accounts.

Here are some of the non-technological tactics used in combination with technological ones:

Administrative regulations to control online magazines, scan mobile phone text messages, require Internet/blog address registers to use real names, and so on. Various government agencies have issued many directives to control particular types of Internet media, organizations, and usage, including online magazines, website registrations, interactive forums and bulletin board services, blogs, and video websites.

The “110 cyber police” on webpages. The cyber police patrol often appears as images of policemen or links for readers to click. They facilitate reporting of “illegal or unhealthy” contents on webpages.

A point system to punish Internet media for infractions. Companies that accumulate points may have their registration licenses suspended or pay hefty fines. Through a complex system of administrative incentives and punishments, the government coerces companies into practicing self-censorship—to filter sensitive contents, block or delete articles, or close down websites and blogs on their own sites.

A “vigilant informants network” with paid cyber patrol men to collect information on “netizens” (persons active in cyber communities), and to infiltrate and sabotage websites or online interactive sites frequented by dissidents/activists.

Continued government use of the criminal law to prosecute Internet users for expressing their views online.

In one extreme case, shutting down the Internet and cell phone networks for the entire Xinjiang Autonomous Region after a riot last July. As of last month, only a couple of official websites had been made accessible.

Google acted in response to hackers breaking into human rights activists’ email (gmail, Yahoo, hotmail) accounts and into Google’s own web database holding users’ passwords, but such reactions are overdue since hacking emails has been an ongoing reality for several years. Typically, the hackers would enter somebody’s email account and send emails to all on the user’s address list, spreading rumors or sending attachments containing viruses. One would receive “important messages” from so-called Google Administrators alerting the user that “due to irregular actions in your account, it will be soon closed” and so on, trying to prompt the user to click a link or open an attachment. But the senders’ addresses, upon inspection, may end with “.tw” or “.ho”. These are clearly fake email addresses, and such emails cannot come from Google. Those who are less experienced might be tricked. Curiously, such hacking seems to target activists rather than random victims. Many in the Chinese activist community, inside China or in exile, have been victims of routine email hacking so much so they rarely communicate anything “sensitive” via emails.

To acknowledge that its company site was hacked and voice its protest, Google put its business in China in jeopardy. Other Internet companies that have suffered the same sort of attack (about 30 of them) have remained silent for fear of losing business in China. Google found its courage to speak up, but its action to pull out of China also raises important ethical questions, as indicated above, about the moral standing (and irony) of American companies doing their part in assisting Internet censorship. It is worthwhile that Google raised such issues and sounded the alarm, while the other Internet companies who have bowed their heads low have apparently gone on with their collaboration with censorship. The repercussions of the Google action, including a televised speech on Internet freedom by Hilary Clinton, the US Secretary of State, in January, did some good by igniting public discussions about corporate responsibilities in the era of globalization of Internet technology. These complex

issues include: when the laws and practices in a foreign country are at odds with our own laws and constitution, and with international norms, does an American corporation have any obligations (legal or moral) to disobey such errant local laws/regulations when doing business there? What does such an obligation entail? Does it require that the corporation forgo profitable market opportunities if they come with the condition to obey such errant laws?

Google’s announcement raised the ethical bar for doing business in an authoritarian police state and put other US Internet companies in a moral conundrum. For example, do the revenues for Yahoo in China really trump Yahoo’s interest in maintaining a clean reputation or the peace of conscience of its CEOs? Yahoo’s reputation nosedived after it was exposed for handing over email records to Chinese police, which resulted in the imprisonment of several Internet writers and journalists. One of them, Shi Tao, is serving a ten-year sentence for leaking “state secrets” through his Yahoo email. Microsoft’s reputation also suffered after it was exposed for shutting down the blog of the Chinese journalist Zhao Jing, who had written and posted an

When the laws and practices in a foreign country are at odds with our own laws and constitution, and with international norms, does an American corporation have any obligations (legal or moral) to disobey?

article about the government’s censoring of a Beijing newspaper. Unfortunately, most foreign Internet companies are so infatuated with their vision of selling products and services to a significant fraction of 1.3 billion consumers that they write off the losses to their reputation and overlook the fact that significant market shares have gone to Chinese companies. Thus, as of today, every page on the MySpace China site includes a link allowing users or monitors to “report inappropriate information” to authorities, and Apple’s iTunes forbids Chinese users to download applications that refer to the Dalai Lama.

It may be true that the majority of China’s nearly 400 million Internet users may not search for such words as “Tiananmen,” “Falun Gong,” or “Dalai Lama.” But if anyone ever does, Google.cn and other foreign Internet (website, blog, email) providers doing business in China have helped the Chinese government to make the information unavailable to that person. And the Chinese government’s increasingly long list of “sensitive” words for Internet blocking suggests that more and more people might be searching for these words, which is the only plausible explanation for the



(Xhacker, Creative Commons Attribution)

expanding official list. The skewed search results, in addition to the government's richly endowed Internet blockage—the Great Firewall—of “sensitive” information online can only contribute to the further distorted views and perspectives of the ordinary Chinese users.

An answer to the question “Will Google’s pullout be a loss to Chinese users?” is thus mixed: yes and no. Since Google searches had only delivered Chinese users skewed and selective information about impor-

An answer to the question “Will Google’s pullout be a loss to Chinese users?” is thus mixed: yes and no.

tant historical and political issues, it’s hardly a loss to have one less distorted search engine. As Google pulls out of mainland China and diverts all searches on google.cn to google.hk, general users still can’t find certain information there anyway and they still can only find government-sanitized information from search results coming out of google.hk since all search results are filtered, from whichever search engines are operat-

ing in China. Cleansed search results are always available on Chinese website portals like Baidu.

Will Google’s pullout have any huge impact on online activists? Hardly. Whether Google.cn stays or leaves, most activists, as long as they remain behind the Great Fire Wall, must “climb over” by employing proxy servers to use uncensored search engines and access open information. Those netizens who are insatiable for information and online activists who have a penchant for alternative (uncensored) information are unlikely to have less access to information and to Google tools, such as Google Document, Google Translation, Gmail Groups, etc., since most of them are already gaining access to the open Internet via proxy servers—one of the most useful tools for bypassing the Great Fire Wall. Users inside the Wall can connect to such a server, which is based outside the Wall, which enables them to visit the open Internet, including all the officially blocked websites.

Chinese online activists and even Chinese IT company professionals are both delighted and saddened by Google’s announcement. One website portal owner was the first to lay flowers in front of Google’s Beijing headquarters upon learning Google’s decision to leave. Chinese netizens commiserated in online chat-rooms and on social sites, saying that foreign compa-

nies can pack up and leave if they are fed up, but where could they go to escape censorship? A card attached to a bunch of flowers reads, "Google [acted like] a real man." Yet another Tweeted: "It is not Google leaving China: It's China leaving the world!" Chinese consumers have a taste for forbidden fruits—banned books, movies, or unavailable (pirated) brand-name designer handbags or CDs often become hot items. Upon learning about the "forbidden" Google tools for open information and free communication—gmail, Google document, translation, etc.—consumers will inevitably have stronger desires than before to get their hands on them, which is what gives substance to Google's otherwise largely symbolic move.

Even if the Chinese government's Internet censorship is mostly furnished by American companies, Chinese users have no doubt benefited from American technology. The technological Trojan horse has worked

The hope for a future of free expression and open information in China lies in these versatile netizens and determined gravediggers of cyber censorship.

both ways. But any credit for the benefits to users does not necessarily go to foreign companies that have entered China by adopting self-censorship. Rather, those Chinese who have the will to undermine censorship have made creative use of Internet tools. The hope for a future of free expression and open information in China lies in these versatile netizens and determined gravediggers of cyber censorship. They are very vocal in denouncing cyber censorship and demanding Internet freedom. They have become very creative in using the new online media to mobilize actions and undermine the Great Fire Wall. For example, though Twitter is blocked in China, after China closed down the popular Chinese social networking site Fanfou last September, many users switched to Twitter and found their way to access the site by proxy

or alternative links. Today, Twitter has become one of the most effective tools for networking and mobilization of Chinese activists. A recent protest against the construction of a waste-processing station was entirely organized and followed on Twitter. In another example, in January, when the government began implementing a new regulation to scan text messages and suspend users' accounts if "illegal, unhealthy" contents are discovered, many Chinese users repeatedly texted censored words in order to overwhelm the censors.

It is hard to know how many Chinese netizens are served by technologies useful for outsmarting cyber censors—how many are using available tools to access the open Internet to engage in digital disobedience and online activism—but the number must have grown to such an extent that the Chinese government has invested billions of dollars to buy technologies and hire companies from the US, of all places, to strengthen its blockage in what is known as the "Golden Shield Project" while deploying a huge troop of cyber police to patrol, monitor, or shut down increasingly more websites, blogs, and social networking sites.

Google's act, whether out of conscience or market strategy, may have not made much of a dent in Chinese cyber censorship. However, desire for freedom of expression and access to information, once aroused, has its own way: the more draconian the measures a government takes to censor the Internet, the more innovative the netizens become, and the more of them manage to find their channels to access online tools to undermine censorship. In this game between a fat cat vying for superpower status and millions of mice, there may have not been a clear winner yet, but the price of controlling millions of mice is growing increasingly high. Google's act has the effect of raising that price.

Xiaorong Li
Institute for Philosophy and Public Policy
lix@umd.edu

