

Google, China, and Search
By Molly Beutz Land

I. Introduction



Google's recent decision to stop censoring its search results in China reflects the challenging position in which providers of information and communication technologies find themselves today. This Insight provides an overview of the debate about Google's provision of search services in China and describes the framework of corporate social

responsibility that applies to Internet providers operating in countries that restrict expression online.

II. Internet Regulation in China

China uses a combination of technological, legal, and social levers to maintain control of online content. The most well-known of these is the "Great Firewall of China." The government requires state-licensed Internet service providers (ISPs), which operate the gateways through which Internet content travels into China, to filter certain identified domain names and URLs, thus preventing them from being accessed by users in China. The resulting bottleneck creates delay and makes pages difficult to load for websites hosted outside the Great Firewall, including Google's main search site, *google.com*.

For content originating within China, the government uses a variety of other techniques. For example, it licenses and regulates ISPs and Internet content providers (ICPs, including all websites with Chinese domain names) and prohibits the transmission or display of prohibited content. This "intermediary liability" means that providers must monitor and police their sites and services in order to maintain their licenses. Although it may order ISPs and ICPs to take down specific content, the government refrains from precisely specifying prohibited content in advance. As a result, many companies generate their own lists of prohibited words and sites, which results in over-blocking. The government also prohibits individual posting of prohibited content and detains and prosecutes violators. Finally, it affirmatively manages online content, allowing the disclosure of some information and relying on coverage provided by state news agencies.^[1]

Although the government's control of the Internet is effective, it is not absolute. Chinese users have access to considerable online content, including some politically sensitive content. By allowing some freedom online, China is able to control content that is of most concern while at the same time largely avoiding discontent that might become a call for political change.^[2]

III. Google's Foray Into China

Google established a subsidiary in China in 2005. On January 27, 2006, Google announced that it was launching *google.cn* as a search engine operating from servers located in China, inside the Great Firewall. The company explained that in order to offer this faster and more reliable search engine on servers in China, "we have agreed to remove certain sensitive information from our search results."^[3] Google made two strategic choices at the time. First, worried that it might be required to share information on Chinese servers with the government, Google would not offer email or blogging tools in China until it was sure it could protect the privacy of individual users. Second, it would inform users when search results had

[Click here to become an ASIL member](#)

RELATED ASIL INSIGHTS

[The Anti-Counterfeiting Trade Agreement in the Public Eye](#)

[Congress Continues to Attack Currency Manipulation as China Defuses G-20 Pressure For Now: the International Law Issues](#)

[Chinese Import Restrictions on Publications and Entertainment Products Found to be WTO Inconsistent](#)

[WTO Panel Report on Consistency of Chinese Intellectual Property Standards](#)

[WTO Softens Earlier Condemnation of U.S. Ban on Internet Gambling, but Confirms Broad Reach into Sensitive Domestic Regulation](#)

[Manipulation of Exchange Rates in International Law: The Chinese Yuan](#)

[Insights Archive>>](#)

DOCUMENTS OF NOTE

[Global Network Initiative Principles](#)

ORGANIZATIONS OF NOTE

[Global Network Initiative](#)

Copyright 2010 by The American Society of International Law ASIL

The purpose of ASIL Insights is to provide concise and informed background for developments of interest to the international community. The American Society of International Law does not take positions on substantive issues, including the ones discussed in this Insight. Educational and news media copying is permitted with due acknowledgement.

The Insights Editorial Board includes: [Cymie Payne](#), UC Berkeley School of Law; [Amelia Porges](#); and [David Kaye](#), UCLA School of Law. [Djurdja Lazic](#) serves as the managing editor.

been censored.

Perhaps because of tension with its informal company motto, “Don’t Be Evil,” Google was roundly criticized for agreeing to comply with Chinese content restrictions. The debate led to congressional hearings before a House subcommittee, where executives from Yahoo!, Google, Microsoft, and Cisco were taken to task for their compliance with Chinese Internet censorship.^[4] It also prompted renewed attention to U.S. legislation designed to regulate companies operating in countries that engage in censorship.

IV. Google’s About Face

In January 2010, Google announced that it had “detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google.” This attack targeted the Google email accounts of Chinese human rights activists. Google stated that it was no longer willing to continue censoring its search results on *google.cn*, explaining: “These attacks and the surveillance they have uncovered—combined with the attempts over the past year to further limit free speech on the web—have led us to conclude that we should review the feasibility of our business operations in China.”^[5]

In March, Google made good on its threat and shut down its China-based search engine. *Google.cn* no longer provided general search services from China, but instead automatically redirected users to Google’s Hong Kong site, *google.com.hk*. Although *google.com.hk*—like *google.com*—provides uncensored Chinese-language search to users in China, it is outside the Great Firewall. Unless a user in China uses encryption or other work-arounds,^[6] the filters of the Great Firewall can block searches from inside China as well as access by users in China to individual pages appearing within the search results.^[7]

On June 28, Google announced that it would no longer automatically redirect users to *google.com.hk*. According to Google, conversations with Chinese officials indicated that the redirect was “unacceptable” and that the government would not renew Google’s ICP license.^[8] Instead, *google.cn* would now provide a user-clickable link to *google.com.hk*, in addition to links to Google’s China-based music search, product search, and translation services.^[9] Although the change is not significant in terms of how users experience the site,^[10] it may have provided Google with a better basis to argue that *google.cn* complies with Chinese law. While automatic redirection might have been considered offering uncensored search services in China, the user-clickable link provides a choice, not a service, since it is the user who decides to access *google.com.hk*.^[11] The compromise appears to have been acceptable to the government. On July 9, Google announced that the government had renewed its ICP license.^[12]

V. Corporate Social Responsibility

The debate about Google illustrates some of the challenges for companies operating in countries that restrict online expression. John Ruggie, the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, has called the situation in which companies are called on to comply with domestic law inconsistent with international norms, “[o]ne of the toughest dilemmas companies face.” He noted that companies are often “caught in the middle unless they find ways to honour the spirit of international standards without violating national law.”^[13]

This situation is difficult in part because there are no clear lines distinguishing prohibited from permitted conduct. Censorship of search engine results can violate the right to seek information in a medium of one’s choice. States may limit this right, however, to protect the rights of others and for reasons of national security and public order. Decisions about such limits are intimately bound up with domestic policies. Germany, for example, prohibits Nazi paraphernalia and Holocaust denial and requires ICPs to remove such material from their local sites.^[14] Although this is not to suggest an equivalency between Germany and China in their regulation of the Internet, the indeterminacy of expressive rights does mean that such distinctions can be difficult to draw. Even jurisdictions that are largely rights-respecting can make demands that violate individual rights.^[15]

This dilemma is compounded by the limited choices available to companies

in this situation and the increasingly significant role they are being forced to assume in controlling content they host and transmit. Companies faced with conflicting demands usually have only two choices, “business as usual” or leaving the country, a choice that may itself have harmful consequences. In addition, the global trend toward increased intermediary liability means that significant responsibility for Internet policy is being outsourced to private companies. Although intermediary liability may be necessary to effectively protect individual rights in some instances, it is also associated with problems of accountability and transparency, as decisions about prohibited content are delegated to private entities not a part of the political process.

VI. Code as Law

These challenges indicate the need for the development of more specific global standards regarding corporate responsibility and online expression. Yet given the range of interests states can have in controlling Internet content, concrete substantive standards may be difficult, if not impossible, to achieve. Nor can regulation be technology-specific, as is the case with prohibited weapons, since information and communication technologies can be used equally for legitimate and illegitimate ends.

One option to explore might be technological standards. Larry Lessig’s well-known maxim, “code is law,”^[16] is instructive here. “Code”—the technological instructions that tell our devices how to function—can restrain behavior as effectively as legislative and judicial rules. (For example, the code that prevents downloading songs onto too many devices can be as effective at preventing music sharing as the threat of civil or criminal penalties.) Although code may also need to be backed up by law (“legal code”) at times, it does provide a set of default assumptions that can have significant effects on conduct.

On the international level, we need to think much more thoroughly about the extent to which our technological standards reflect policy choices. Ethan Zuckerman, for example, has encouraged companies to build their platforms in ways that make them difficult to censor, noting that if YouTube increased the number of internet protocol addresses leading to its site, the site would be more difficult to block.^[17] Code can also be built into technological standards. China, for example, has unsuccessfully pushed for wireless standards that would have prevented users from logging on to networks anonymously, and it has tried to require installation of filtering software on personal computers sold in China.^[18] We need to consider the policies embedded into our standards and platforms as carefully as we consider those built into law.

VII. The Global Network Initiative

Given the indeterminacy of online rights, the work of the Global Network Initiative is a welcome development. The Initiative is a multi-stakeholder effort aimed at generating principles for information and communication technology companies faced with pressure to comply with domestic laws that are at odds with international standards. With only three companies signed on to its principles, Google, Yahoo, and Microsoft, the Initiative is still in its early stages, but its principles do suggest possible directions.

The Initiative’s principles call on participating companies to “avoid or minimize” the impact of government restrictions on freedom of expression and to “respect and protect the freedom of expression rights of their users” when faced with contrary domestic legislation.^[19] Implementation guidelines encourage companies to engage with the host government on Internet policies, clarify and narrow government requests, minimize the negative effects of compliance, challenge regulations believed to violate international law, and be transparent with respect to any actions taken in compliance with such regulations.^[20]

Although the principles are an important step, they also pose risks. First, there is a risk that superficial compliance with the principles might provide cover to companies seeking to do business in restrictive regimes. Second, the principles’ ambiguity means that companies have to exercise judgment and imagination in responding to demands to follow local law. Third, there may be few incentives for companies to engage with local governments or to invest the resources needed to achieve long-term change.^[21]

Google’s negotiation with the Chinese government provides an opportunity

to evaluate the principles in action. By providing a link to an uncensored search engine elsewhere, Google attempted to interpret Chinese regulations narrowly and minimize the harm to users. In order to stop censoring its search results, however, Google had to shut down its China-based search engine. In addition, the censorship experienced by users of *google.com.hk* is in some ways less transparent than previously encountered on *google.cn*. Instead of receiving results with a message that some entries were removed to comply with local law, searches and individual pages are simply unavailable.

At the same time, providing a link to an uncensored search engine on a website in China encourages more access than if individuals had to seek out *google.com.hk* on their own. Censorship via technological filters also tends to be more porous than ICP self-regulation. Most important, however, has been the dialogue between Google and the government. Google has proactively sought clarification about the requirements of Chinese law and challenged requests that it believed were inconsistent with international norms. Over time, this type of engagement is critical in fostering the long-term change that the principles seek to achieve.

Google's recent exchange with China also indicates that, at least with respect to the Internet, there may be more alignment between business incentives and corporate social responsibility than might be assumed. Public pressure on Google certainly played an important role in its decision to change its business practices. Yet human rights and rule of law can have additional consequences for a company's business model. States that do not respect the privacy of their citizens' information are unlikely to respect that of companies operating within their borders. For information and communication technology companies, infrastructure security is a critical component of their business model. As a result, it may become increasingly difficult for companies to remain agnostic about the information and communication policies of the countries in which they operate.

About the Author

Molly Beutz Land, an ASIL member, is an Associate Professor of Law at New York Law School, where she focuses her scholarship on access to knowledge and the intersection of technology, intellectual property, and human rights. Her recent work examines the participatory potential of technology to broaden the mobilization of ordinary citizens in human rights advocacy.

Endnotes

[1] See generally *China's Information Control Practices and the Implications for the United States*, *Testimony Before the U.S.-China Econ. & Sec. Review Comm'n* (June 30, 2010) (testimony of Rebecca MacKinnon, Visiting Fellow, Ctr. for Info. Tech. Policy, Princeton Univ.), http://www.uscc.gov/hearings/2010hearings/written_testimonies/10_06_30_wrt/10_06_30_mackinnon_statement.php [hereinafter *MacKinnon Testimony*]; JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006); HUMAN RIGHTS WATCH, "RACE TO THE BOTTOM": CORPORATE COMPLICITY IN CHINESE INTERNET CENSORSHIP (2006), available at <http://www.hrw.org/en/reports/2006/08/09/race-bottom>; OPENNET INITIATIVE, INTERNET FILTERING IN CHINA (2009), available at http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf; *China (Including Hong Kong)*, in ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 263 (Ronald Deibert et al. eds., 2008); Clive Thompson, *Google's China Problem (and China's Google Problem)*, N.Y. TIMES MAG., Apr. 23, 2006, available at <http://www.nytimes.com/2006/04/23/magazine/23google.html>.

[2] *MacKinnon Testimony*, *supra* note 1, at 2.

[3] Andrew McLaughlin, *Google in China*, OFFICIAL GOOGLE BLOG (Jan. 27, 2006, 11:58 AM), http://googleblog.blogspot.com/2006_01_01_archive.html; see also Thompson, *supra* note 1.

[4] Cisco was criticized for selling routers and other hardware that the Chinese government used to monitor and filter the Internet and for helping the government develop its proxy server system. Microsoft was accused of censoring and shutting down blogs with politically sensitive content and of

censoring its search engine, while Skype's Chinese subsidiary had built censorship functions into its chat client. Yahoo!China was criticized for providing information to the Chinese government that led to the conviction of four dissidents, an action that led to a lawsuit against Yahoo! under the Alien Tort Statute. Google was criticized for *google.cn*'s search filtering. See generally HUMAN RIGHTS WATCH, *supra* note 1, at 6, 15-16; Verne Kopytoff, *New Charge Yahoo Aided China Crackdown: 4th Dissident Jailed with Online Data, Rights Group Says*, S.F. CHRON., Apr. 29, 2006; Thompson, *supra* note 1; Jim Yardley, *Google Chief Rejects Putting Pressure on China*, N.Y. TIMES, Apr. 13, 2006; Nicholas D. Kristof, *China's Cyberdissidents and the Yahoos at Yahoo*, N.Y. TIMES, Feb. 19, 2006; Joe Nocera, *Enough Shame to Go Around on China*, N.Y. TIMES, Feb. 18, 2006; Tom Zeller Jr., *House Member Criticizes Internet Companies for Practices in China*, N.Y. TIMES, Feb. 15, 2006.

[5] David Drummond, *A New Approach to China*, OFFICIAL GOOGLE BLOG (Jan. 12, 2010, 3:00 PM), <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>; see also *Google 'May Pull Out of China After Gmail Cyber Attack'*, BBC NEWS, Jan. 13, 2010, available at <http://news.bbc.co.uk/2/hi/8455712.stm>.

[6] See Rebecca MacKinnon, *On Google's License Renewal and Principled Engagement*, RCONVERSATION (July 9, 2010, 4:49 PM), <http://rconversation.blogs.com/rconversation/2010/07/on-googles-license-renewal-and-principled-engagement.html> (describing how users can encrypt their Google searches by adding an "s" to the "http" in the address bar to access an "encrypted function that make[s] your searches invisible to the Chinese network operators").

[7] See Miguel Helft & David Barboza, *Google Shuts China Site in Dispute Over Censorship*, N.Y. TIMES, Mar. 22, 2010; Jillian C. York, *Google.cn Redirects to Hong Kong . . . For Now*, OPEN NET INITIATIVE BLOG (Mar. 25, 2010, 5:58 PM), <http://opennet.net/blog/2010/03/googlecn-redirects-hong-kongfor-now>.

[8] David Drummond, *An Update on China*, OFFICIAL GOOGLE BLOG (June 28, 2010, 10:45 PM), <http://googleblog.blogspot.com/2010/06/update-on-china.html> [hereinafter Drummond, *An Update on China*]; see also Brad Stone & David Barboza, *Google to Stop Redirecting Chinese Users to Hong Kong*, N.Y. TIMES, June 29, 2010.

[9] *Google's ICP License Renewed, and ISP Liability Released*, BLAWGDOG (July 20, 2010, 5:37 AM), <http://english.blawgdog.com/2010/07/googles-icp-license-renewed-and-isp.html>.

[10] See MacKinnon, *supra* note 6.

[11] See *Google's ICP License Renewed*, *supra* note 9; see also Brian Womack & Mark Lee, *Google Wins Renewal of Its China License, Xinhua Says*, BLOOMBERG BUSINESSWEEK, July 22, 2010, available at <http://www.businessweek.com/news/2010-07-11/google-wins-renewal-of-its-china-license-xinhua-says.html> (reporting a statement by the government that it had renewed Google's Internet license after Beijing Guxiang Information Technology Co., the joint venture between Google and a Chinese firm that holds the ICP license for *google.com*, promised to comply with Chinese law and refrain from providing prohibited content). As Rebecca MacKinnon argues, the government may have welcomed the compromise as a way of sending a positive message to the international business community, avoiding questions about censorship as a trade barrier, and fostering the foreign competition necessary for domestic innovation. MacKinnon, *supra* note 6; see also Womack & Lee, (noting that "[l]etting Google keep operating may help the government show it's open to outside competition").

[12] Drummond, *An Update on China*, *supra* note 8 (updated July 9, 2010); see also David Barboza, *China Renews Google's License*, N.Y. TIMES, July 9, 2010 (providing image showing that the ICP license number (B2-20070004) appears below the search box on <http://www.google.cn>). The links on *google.cn* do not include *ditu.google.cn*, the Google Maps China site, which is still under review. See Thomas Claburn, *Google Confronts Map Censorship*, INFO. WEEK, July 13, 2010, <http://www.informationweek.com/news/storage/security/showArticle.jhtml?articleID=225800001>.

[13] Special Representative of the Secretary-General, Business and Human Rights: Towards Operationalizing the “Protect, Respect and Remedy” Framework, Rep. of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and other Business Enterprises, ¶¶ 66-67, U.N. Doc. A/HRC/11/13 (Apr. 22, 2009).

[14] See Jonathan Zittrain & John Palfrey, *Internet Filtering: The Politics and Mechanisms of Control*, in ACCESS DENIED, *supra* note 1, at 29, 41.

[15] See Rebecca MacKinnon, *Global Internet Freedom and the U.S. Government*, FREEDOM TO TINKER (Mar. 15, 2010, 11:27 AM), <http://www.freedom-to-tinker.com/blog/rmackinnon/global-internet-freedom-and-us-government> (arguing against designating certain countries as “Internet Restricting” because “while I am not drawing moral equivalence between Italy and Iran I do believe there is no country on earth, including the United States, where companies are not under pressure by government agencies to do things that arguably violate users’ civil rights”).

[16] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

[17] Ethan Zuckerman, *Internet Freedom: Beyond Circumvention*, MY HEART’S IN ACCRA (Feb 22, 2010, 7:27 PM), <http://www.ethanzuckerman.com/blog/2010/02/22/internet-freedom-beyond-circumvention>.

[18] See OPENNET INITIATIVE, *supra* note 1, at 21 (on Green Dam software); GOLDSMITH & WU, *supra* note 1, at 101 (on WAPI standards).

[19] Global Network Initiative, Principles on Freedom of Expression and Privacy at 2.

[20] Global Network Initiative, Implementation Guidelines for the Principles on Freedom of Expression and Privacy at 4-7.

[21] See generally Dan Levin, *New Scrutiny on Censorship Issues for U.S. Companies in China*, N.Y. TIMES, Mar. 2, 2010 (noting that Arvind Ganesan, director of the business and human rights program at Human Rights Watch, acknowledged that the “Global Network Initiative would be meaningless if companies cited their participation in the framework but failed to push actively for a more open Internet while expanding operations in countries like China”).