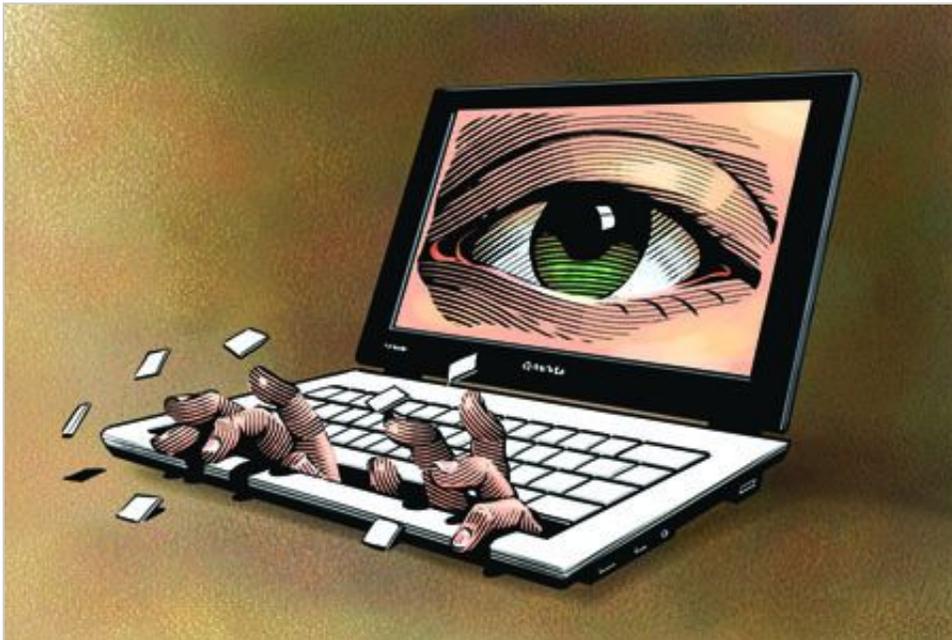


April 2008

Asia's Fight for Web Rights

by Rebecca MacKinnon

In November 2007, Yahoo! Inc. did what it could have done two years ago when it became known that the company had aided the 2005 conviction of Chinese journalist Shi Tao, now serving 10 years in prison for "revealing state secrets." In a legal settlement, Yahoo pledged to provide an undisclosed amount of "financial, humanitarian and legal support" to the families of Shi Tao and Wang Xiaoning, another dissident jailed in 2003 for 10 years with the help of email data supplied by Yahoo. This came immediately after Yahoo cofounder and chief executive officer, Jerry Yang, made a dramatic public apology to Shi Tao's mother, Gao Qinsheng, at a United States Congressional hearing. He bowed solemnly to her three times as tears rolled down her cheeks.



This January, the company went even further, setting up a "Yahoo! Human Rights Fund" to be administered by human-rights activist Harry Wu to "provide humanitarian and legal assistance to persons in the People's Republic of China who have been imprisoned or persecuted for expressing their views using the Internet." Mr. Yang convinced Condoleezza Rice to raise the cases of Messrs. Wang and Shi with Chinese leaders on a trip to Beijing in February. Meanwhile, according to Yahoo executives, human-rights assessments are now conducted before entering sensitive markets or launching new products in those markets. The company is also an active participant in a "multistakeholder process" to establish a global code of conduct on free expression and privacy for Internet and telecommunications companies.

These are all positive steps, but getting to this point has been a painful journey. The company had to be called on the carpet twice by the U.S. Congress, denounced by human-rights groups and condemned by journalists around the world in support of Shi Tao.

How might Yahoo have avoided complicity in the conviction of Chinese political dissidents in the first place? The answer brings sobering lessons for all Internet and telecommunications companies. Many would agree that being a socially responsible Internet or telecommunications company requires respect for users' rights to privacy and free expression, but there is great disagreement over how to accomplish this ideal.

Evil or Negligent?

Shi Tao's case was the last of Yahoo's four known data-handover cases in China. Wang Xiaoning, plus two other dissidents Li Zhi and Jiang Lijun, were all convicted with Yahoo's help in 2003. But the Shi Tao case became public first, had more details associated with it and has provoked the greatest amount of international controversy. It thus highlights many of the thorny privacy challenges that Internet companies face in China and around the world.

At the time of his arrest, Mr. Shi worked for Dangdai Shangbao (Contemporary Business News), based in Changsha, Hunan province. In April 2004, he attended an editorial meeting to discuss a classified document containing a series of instructions about how the media should work to prevent social unrest in the run-up to the anniversary of the June 4, 1989 crackdown. Later that night he wrote up his notes summarizing the document and sent them from his office computer via his Yahoo China email account to a New York-based, pro-democracy publication and Web site, Minzhu Luntan (Democracy Forum), which published his article under a pseudonym.

Two days later, the Beijing State Security Bureau issued a "Notice of Evidence Collection" to Yahoo's Beijing office, requesting account information linked to Mr. Shi's email address (which did not contain his name), plus contents of his emails. Beijing-based employees of Yahoo China complied with the request. Mr. Shi was detained and arrested at the end of 2004 and charged with "leaking state secrets." His trial in March 2005 lasted two hours, resulting in a guilty verdict and 10-year prison sentence. In September that year, a copy of the court verdict was obtained and translated by the San Francisco-based Dui Hua Foundation, and then published on the Web site of Reporters Without Borders. Among the evidence it listed "Account holder information furnished by Yahoo Holdings (Hong Kong) Ltd.," including his office computer's Internet protocol address and his office address.

In response to an outcry in Hong Kong about the role of a Hong Kong-based entity, Hong Kong's Privacy Commissioner held an investigation, and

concluded that Shi Tao's data had always been located on computer servers in mainland Chinese jurisdiction, and therefore no Hong Kong privacy laws had been broken. Yahoo had launched its Hong Kong operation in January 1999 and set up a Beijing office later that year, unveiling a simplified Chinese-language portal that included a search engine, email and instant messaging services. Until the Chinese company Alibaba Group assumed full operational control over all "Yahoo China" operations in late 2005, Yahoo China's business license was officially registered in the name of Yahoo (Hong Kong) Holdings. Actual operations of Yahoo China were conducted in mainland China by two mainland-China-based entities: Yahoo Beijing and the Peking University Founder Group Corp.

Corporate Responsibilities And Realities

For two years after Yahoo's role in Shi Tao's case first came to light, the company's public statements characterized the plight of Shi Tao and the three others as if they were acceptable collateral damage in the great task of bringing Internet information services to the Chinese people. Executives argued that the Chinese people were still better off in the long run thanks to Yahoo's presence. In 2006, Mr. Yang said, "we have no way of preventing that beforehand... If you want to do business there you have to comply." It was as if Yahoo had only two choices: leave China or roll over and play dead.

Yahoo executives also argued that the company's nose was legally clean on two fronts: Not only did employees respond to a legally binding written order; actions by Yahoo's China-based employees were consistent with the user "terms of service" that Shi Tao and all other Yahoo email users agree to in order to create an account. In these terms the user promises not to use the email account to commit a list of actions, including "damaging public security, revealing state secrets, subverting state power, damaging national unity," etc. The same document, to which Mr. Shi technically agreed (regardless of whether he actually read or understood it), acknowledged that his information would be disclosed if required to do so by law.

For these two reasons it is possible that if the families' lawsuit against Yahoo had proceeded in U.S. court, Yahoo may have prevailed. But a legal victory would have been hollow because it would not have absolved Yahoo in the eyes of the human-rights community and socially responsible investors. They point out that Chinese law in this area contradicts international law—and that socially responsible companies have an obligation to do something more than participate in a "race to the bottom" as far as global practices on privacy and freedom of expression are concerned.

After much public pummeling, Yahoo management eventually came to acknowledge that companies can and do make choices all the time not only about whether to do business in a particular market, but also how to do

business there, and what products and services are appropriate given the nature of that market's controlling government.

Yahoo was the first major U.S. Internet brand to enter the China market—Google Inc. and Microsoft Corp.'s online content division, msn, did not establish physical presences in China until nearly six years later. To this day Yahoo is the only foreign brand (though now managed entirely by Alibaba) providing an email service that keeps user data on computer servers inside mainland China. Different business decisions by Google and Microsoft have made Mr. Yang's claims of having "no choice" ring hollow. A more honest statement was that Yahoo as first mover made the bulk of the mistakes that competitors would learn from.

Microsoft and Google say they have no plans to follow in Yahoo's footsteps with localized Chinese versions of their respective email products, Hotmail and Gmail: executives from both companies have been candid about not wanting any more Shi Taos on their hands. msn and Yahoo both provide localized Chinese blogging platforms: Yahoo Chinese blogs are censored to a similar degree as other domestic Chinese blog-hosting services, while msn now censors very little—after a major international uproar over its deletion of a controversial Chinese blog on authorities' request in late 2005.

Google has chosen not to provide that particular service in China. All three companies do offer censored search engines in China—with Yahoo China censoring the most, msn China a bit less and Google.cn censoring substantially less than Yahoo China. This observation is based on tests I conducted for a 2006 Human Rights Watch report on corporate complicity in Chinese Internet censorship: I ran Chinese-language searches across all three search engines plus Baidu, using a range of phrases on a variety of subjects with varying political sensitivity. The relative degree to which the three censor search results in China has not changed much since then.

Much has recently been written by journalists and academics about the mechanics of Internet censorship and search engine censorship in China, and there has been much debate over the ethics of providing a censored search engine of any kind, even if it does censor less than the local competition. Some believe it's unacceptable to comply with any political censorship demands, while others focus on the need to be more transparent with users about what is being censored, on whose authority and according to what process, so that users can be better informed of the skewed information picture the service is providing. How to deal with government censorship demands in an ethical and honest manner is an important debate. Satisfactory solutions that would enhance overall freedom of expression are difficult to pin down—mainly because there is disagreement about how censorship impacts the lives of individuals. With data privacy, things are much more clear cut: when user data is handed over a person can go to jail and his or her life is ruined or shortened. So what to do?

Toward a Solution

Debates about what Internet companies should or shouldn't do with user information tend to focus on combinations of four different options:

**Selective compliance option.* Companies should comply with government information requests only in truly criminal cases and refuse to cooperate in cases involving political dissent

**Offshore option.* Companies should not host important user information on computer servers inside a jurisdiction such as the PRC, whose definition of "crime" is well known to include political activities and speech

**Minimal data option.* Companies in any jurisdiction should retain the minimum amount of personally-identifying user data for the minimum amount of time necessary to provide a particular service

**Strong warning option.* While a company may cover its legal obligations with existing terms of service, it has a moral obligation in jurisdictions such as the prc (or arguably anywhere) to make explicit to users where their data is being stored and how it may be used.

Shi Tao and others may have had a false sense of security when choosing to use email accounts with an American brand-name attached. All or some of these four options form the basis for different solutions advocated by different groups:

* **Lawmakers.** In early 2006 members of the U.S. House of Representatives introduced a bill called the Global Online Freedom Act. Sponsored by Rep. Chris Smith (R-NJ), the proposed legislation was reintroduced in 2007 and passed all the required committees this past February. In its current form, GOFA would require U.S. companies to adhere to all four options described above in their approach to data-privacy issues when operating in any "internet restricting country" —as designated by the President. (For nondesignated countries, it's business as usual.) In cases where companies are asked to hand over data, the U.S. Department of Justice would decide what does or doesn't constitute "legitimate law enforcement purposes." Companies would also be required to report to the U.S. State Department all keywords and Internet addresses that designated governments require them to censor. Victims of U.S. company data disclosure would be able to sue the companies in U.S. court more readily, and noncompliant companies could be fined up to \$2 million. Rep. Smith now plans to take the bill to a full House debate and vote, although a time has yet to be scheduled. So far no similar bill has emerged in the Senate.

Critics of the bill point to several problems. Danny O'Brien of the Electronic Frontier Foundation, a free speech group, has pointed out that the bill treats companies as "enemies to be controlled and puts them in the middle of a 'fight between the U.S. government and other governments.'" Others

(including myself) have been critical of an approach that would divide the world into "good" and "bad" countries according to Washington's view of the world. There is no country on earth where Internet and telecommunications companies do not face at least some pressure from governments to do things that would potentially infringe on users' rights to free expression and privacy.

* **Activists.** GOFA was drafted in consultation with several human-rights groups—some though not all of which advocate all four options above. The bill has been endorsed by 16 human-rights groups including Human Rights Watch, Amnesty International, Reporters Without Borders and the Committee to Protect Journalists.

In 2006, Reporters Without Borders, Amnesty International, and Human Rights Watch all published recommendations for how Internet companies might engage with the China market in a more socially responsible way. Reporters Without Borders advocated all four options, with a strong role for the U.S. government in monitoring and supervising company relations with governments of "repressive countries." Human Rights Watch recommended versions of all four options, but with an emphasis that if user data is kept offshore the selective-compliance option might be avoided. Amnesty International took a broader approach, asking companies to develop human-rights policies, "publicly commit to honoring the freedom of expression provision in the Chinese constitution," and "exhaust all judicial remedies and appeals in China and internationally before complying with state directives where these have human-rights implications" (a more flexible form of the selective compliance option than what gofa recommends). All groups called for companies to develop a voluntary code of conduct, support the development of technologies that protect users, and work for policy and legislative change in markets where they operate in ways that favor their users' rights.

* **Investors.** Investors concerned about corporate social responsibility have been asking tough questions about companies' labor and environmental practices for decades. But the free-speech and privacy aspect of corporate social responsibility did not hit the radar screens of the CSR investment community until about three years ago when shareholders began to bring resolutions against Cisco Systems Inc. for its relationship with Chinese law enforcement in addition to the role played by its routers in the Chinese blocking of many overseas Web sites. In 2007 a shareholder resolution filed by the New York City Comptroller against Yahoo called for "certain minimum standards" involving the offshore option, the minimal-data option, and strong-warning options. No mention of the more problematic selective-compliance option.

The resolution did not pass, nor did a similar resolution against Google calling for greater transparency in how it censors. Both companies advised shareholders to vote against the resolutions. Yahoo management argued

that while they are working to improve their corporate policies on free expression and privacy, the resolutions' "overly prescriptive" and "static" standards would make it hard to do business at all in many markets, and that a more "flexible" approach might in the end be more effective in upholding the spirit of the resolutions.

* **Multistakeholder initiative:** For the past two years, Yahoo, Google, Microsoft, Vodafone, France Telecom and the Swedish telecoms company TeliaSonera, have been participating in a "multistakeholder process" with 24 "stakeholder groups" including the major human-rights groups mentioned above, free-speech organizations, socially responsible investment funds and several academic institutions. (Full disclosure: I am also a participant.) Led by the Washington-based Center for Democracy and Technology and the San Francisco-based Business for Social Responsibility, the aim of the process is to craft a realistic but meaningful set of standards to help Internet and telecommunications companies who want to be socially responsible to uphold core principles of free expression and privacy. The idea is also to set up a workable system for evaluating companies' actions in this area in order to benchmark over time who are the industry leaders and laggards—so that investors and users can make more informed decisions about where to put their money or whose services to use for what purpose. Furthermore, "one size fits all" prescriptions for a range of products, services, technologies and markets are not always the most effective way to achieve privacy and free expression, and can be counterproductive or have unintended consequences. A better way forward may be for all nongovernment stakeholders to agree to a set of common principles, then commit to an on-going process of benchmarking, watchdogging, shared learning, and broader dialogue with society and governments.

The process of bringing these diverse groups to agreement has been difficult and often contentious. The exact content of the drafts under discussion remains confidential but on the issue of data privacy they tend to focus on the minimal data option and strong-warning option, plus a more flexible approach to the offshore option, emphasizing the need for companies to think through the implications of where, how and for how long they store what user data. Final agreement has yet to be reached but participants are hopeful that a meaningful set of principles on free expression and privacy—with mechanisms to measure company adherence, plus a commitment to shared learning and public dialogue—will likely be announced this year. Companies and concerned organizations from any country in the world will be welcome to join. No governments are involved.

Global Issue, Global Standards

The multistakeholder initiative (yet to be named) aims to be truly global, because the problem is global: it is hard to find a country where Internet and telecommunications do not face some pressure from governments to do things that arguably are harmful to free expression and privacy. One of

the admitted problems is that it currently does not include any non-Western companies. It is the hope of many participants that this will change soon after the initiative goes fully public and starts expanding its membership. While it may be difficult for mainland Chinese companies to commit publicly to uphold their users' rights to free expression and privacy, this initiative is not targeted at China or any one country specifically. It is likely that many companies in places like South and Southeast Asia, Hong Kong, South Korea, Taiwan, and Japan will see it in their long-term interest to participate—for the same reasons that companies around the world are increasingly signing up to multistakeholder initiatives committed to environmental protection, sustainable development and basic labor standards.

Information-technology companies everywhere rely largely on user trust for their business success. It is in their interest to join hands in setting industry-wide standards and practices that will minimize harm to their users. Companies in many markets once claimed they would be committing business suicide if they changed their behavior when it came to environmental and labor practices, but have since come round to recognizing that corporate social responsibility is not optional. It's time to make respect for free expression and privacy equally nonoptional.

Thorny problems certainly abound: one involves local subsidiaries of multinationals that make the commitment. Yahoo China, for instance, is now a division of Alibaba. When asked how Yahoo will avoid contributing to the conviction of any more Chinese dissidents, company executives have pointed out that since ownership of Yahoo China was transferred to Alibaba in October 2005, Yahoo Inc. no longer has day-to-day control over the Chinese email and Web services even though they still bear the Yahoo brand name. Yahoo holds one of four seats on Alibaba's board. But it is unclear how much influence they have over Alibaba's relationship with Chinese law enforcement and state security.

All of this is further complicated by recent news of Microsoft's bid to buy Yahoo Inc., followed by a strong rumor, recently reported by Reuters, that Alibaba is seeking investors to purchase Yahoo's 39% stake in Alibaba so that Microsoft will not end up getting the same stake in Alibaba. None of the major Western venture-capital or private-equity investors pouring cash into Chinese Internet companies has shown any sign of trying to influence those companies to maximize their respect for Chinese user rights—even within the constraints of the Chinese system. It's impossible without a very high-level State Security mole to get data on how many dissidents Chinese email service companies have helped to put behind bars. But research I am presently conducting on the way in which Chinese companies censor their users' blog and chat-room postings indicates that there is substantial variation in how different Chinese companies treat their users. To merely say "I have no choice" is oversimplistic in any market.

Meanwhile, the rest of us should not simply sit around and wait for our

Internet and email service providers, Web-hosting services, and mobile-phone carriers to do the right thing on their own. Technology users around the world have an interest in joining together to insist that the products and services with which we increasingly entrust our careers, our beliefs and the most intimate parts of our lives, will not sell us out because they feel they have "no choice" since all their competitors are selling out their users too.

Ms. MacKinnon is an assistant professor at the University of Hong Kong's Journalism and Media Studies Centre. She writes frequently about the Internet, free speech and China at <http://rconversation.blogs.com>. (This article appears in the April 2008 issue of FEER.)