

China

China has devoted extensive resources to building one of the largest and most sophisticated filtering systems in the world. As the Internet records extraordinary growth in services as well as numbers of users, the Chinese government has undertaken to limit access to any content that might potentially undermine the state's control or social stability by pursuing strict supervision of domestic media, delegated liability for online content providers, and, increasingly, a propaganda approach to online debate and discussion.



Background

The convening of the Seventeenth Chinese Communist Party (CCP) Congress in October 2007, at which China's top echelon of government leaders chose their eventual successors, was the beginning of a momentous year for China, and consequently for domestic and international news media. On March 10, 2008, hundreds of monks in the Tibetan autonomous region led a series of protests to demand loosening of restrictions on religious practices and even independence for Tibet.¹ Chinese authorities

RESULTS AT A GLANCE

Filtering	No Evidence of Filtering	Suspected Filtering	Selective Filtering	Substantial Filtering	Pervasive Filtering
Political					•
Social				•	
Conflict and security					•
Internet tools				•	

Other Factors	Low	Medium	High	Not Applicable
Transparency	•			
Consistency			•	

KEY INDICATORS	
GDP per capita, PPP (constant 2005 international dollars)	5,084
Life expectancy at birth (years)	73
Literacy rate (percent of people age 15+)	93
Human development index (out of 179)	94
Rule of law (out of 211)	121
Voice and accountability (out of 209)	196
Democracy index (out of 167)	136 (Authoritarian regime)
Digital opportunity index (out of 181)	77
Internet users (percent of population)	22.6

Source by indicator: World Bank 2009a, World Bank 2009a, World Bank 2009a, UNDP 2008, World Bank 2009b, World Bank 2009b, Economist Intelligence Unit 2008, ITU 2007, ITU 2008.

rapidly responded with arrests and a violent crackdown against thousands of monks and rioting Tibetans.² A corresponding clampdown on reporting from the region and other Tibetan-populated areas in western China left media with a dearth of reliable information; official accounts and dispatches released by Tibetan exile organizations put issues like the actual death toll in question. The crackdown in Tibet galvanized protests both in support of and opposed to China's policies toward its religious and ethnic minorities, especially as symbolized in the Olympic torch making its way in an elaborate tour around the world. The conflicts that erupted in cities as distant as Paris³ and Seoul in March and April contributed to a so-called transnational Chinese backlash against Western media portrayals of China, culminating in an "anti-CNN" movement and a call for a boycott against the French supermarket chain Carrefour.⁴

On May 12, 2008, a 7.9-magnitude earthquake, with its epicenter in Wenchuan county, Sichuan province, killed around 90,000 people and injured hundreds of thousands, leveling more than 5 million buildings and leaving millions homeless.⁵ During the massive relief efforts and national mobilization of volunteers and monetary contributions immediately following the quake, media were allowed to operate with unprecedented openness, with official state outlets such as China Central Television winning notice and praise for presenting timely and uncanned news. However, within a few weeks authorities began to encircle and regulate the story—for example, by issuing more bans on coverage of certain topics and requiring registration of reporters. It took authorities repeated efforts to quash coverage of one of the most potent and enduring controversies: the tragic deaths of thousands of schoolchildren and teachers attributed to shoddy school construction, along with the implication that government officials were responsible.⁶ Authorities did not release an official statistic of the number of schoolchildren who died until almost a year after the quake, and some claimed that the official figure of 5,335 was too low, compared to Reuters' estimate of 9,000 deaths,

calculated from reports by the state news agency and local media.⁷ This accusation led one commentator to state, “Chinese news reports on this major story unfolded in a complicated environment, and it is impossible to render a simple verdict about media coverage.”⁸

With more than USD 40 billion spent on hosting the 2008 Olympic Games in Beijing, the Chinese government acted to assert control over this global event while presenting an open and welcoming environment for athletes, media, foreign dignitaries, and visitors.⁹ As part of these overtures, the government issued regulations in January 2007 allowing journalists to travel across the country without registering with local authorities and to interview subjects without official consent.¹⁰ While the unblocking of Web sites and improved access to officials at Olympics venues marked some improvement in openness and transparency, the government also stepped up surveillance around Beijing and prevented activists from petitioning to use legally sanctioned protest zones.

After a news conference held by the U.S. men’s volleyball team, in which several Chinese reporters had their notebooks (and at least one tape recorder) confiscated, Beijing Olympics spokesman Sun Weide denied knowledge of this differential treatment of Chinese reporters: “I am not very clear about the situation you raised,” he said. “For Chinese journalists, they very much enjoy the rights to cover the Beijing Olympic Games. . . . the rights are protected by the constitution in China.”¹¹ Yet China’s “open-door” policy for journalists as a result of the Olympics had a marginal impact on Olympics coverage by domestic media. The government persisted in its clampdown on local Chinese media,¹² and the Foreign Correspondents’ Club of China confirmed 63 cases of reporting interference during the Olympics, out of a total of 178 in 2008, including ten incidents of police roughing up reporters and breaking their cameras.¹³ While the relaxed rules for foreign journalists were made permanent in October 2008,¹⁴ new rules issued in February 2009 required reporters based in Hong Kong and Macao to apply for a permit prior to every reporting trip to mainland China.¹⁵

A month after the Olympics concluded, a scandal erupted over tainted milk products that killed six infants and sickened nearly 300,000 others.¹⁶ Information soon emerged indicating that provincial governments and central government agencies, as well as officials from the Sanlu group, China’s leading seller of milk powder, had either suppressed earlier reports or failed to act, likely at the cost of human lives.¹⁷ Although it had been receiving complaints about its infant milk powder since December 2007, the Sanlu group only informed its board in August 2008, prompting its joint venture partner Fonterra to inform the New Zealand government.¹⁸ A reporter for the newspaper *Southern Weekend*, known for its investigative reports, wrote in a blog post that he and several other journalists were prevented in July from publishing findings about how milk powder was making children sick because of pressure from Sanlu

officials as well as an overall Olympics-related clampdown on negative news coverage.¹⁹ In January 2009, 21 defendants were convicted for their roles in the production and sale of melamine-tainted products, including two melamine producers, who received death sentences, and the former Sanlu chairwoman, who was sentenced to life imprisonment.²⁰

As 2008 progressed, the Chinese government demonstrated a perceptible shift in its media-control policies in order to better manage the handling of negative news reports, which continued to spread with incredible speed and intensity on the Internet. This approach involves the government responding more actively and rapidly to fast-breaking news events, primarily by attempting to set the agenda for coverage rather than suppress it.²¹ With lessons learned about the upsides of transparency and timeliness from the early Sichuan earthquake coverage and other emergencies, the central government reportedly began allowing local governments to disclose information about unrest and protests in an apparent attempt to “control the news by publicizing the news.”²² However, despite gestures toward broader openness with the media, the government clearly did not intend to relinquish control.²³ This tactic often resulted in the same delivery of “authoritative” facts, with state news agencies such as Xinhua and the *People’s Daily* benefiting over commercial media from this selectively enhanced coverage.²⁴ In February 2009, the official China News Service announced that it would create a blacklist of journalists engaged in “unhealthy professional conduct,” and those found breaking rules would be prohibited from engaging in news reporting and editing work.²⁵

Coming off of these perceived triumphs and devastating crises, the Chinese government warned that extra vigilance was needed in 2009. The potential for increased social instability triggered by the global financial crisis increased anxieties in a year already punctuated by powerful anniversaries of events tainting the legacy of the CCP, which will also commemorate 60 years since the founding of the People’s Republic of China: 20 years since the June 4, 1989, Tiananmen Square crackdown; 50 years since the Tibetan uprising that led to the Dalai Lama’s exile; and ten years since the Falun Gong spiritual movement was banned quickly after their 10,000-strong flash protest in front of Zhongnanhai, the compound of the Chinese central leadership. Thus, officials repeatedly issued reminders that “stability preservation work”²⁶ would be a top priority. At a media forum in January, an official in China’s Internet affairs bureau said, “You have to check the channels one by one, the programs one by one, the pages one by one. . . . You must not miss any step. You must not leave any unchecked corners.”²⁷ Efforts to enforce stability preservation have resulted in predictable crackdowns on media reporting; for example, in March 2009, reporters were detained, turned back, or had their recordings confiscated when trying to visit Tibetan areas in three provinces ahead of the first anniversary of the unrest in Tibet.²⁸

Internet in China

China leads the world with 298 million Internet users, an increase of 42 percent from 2007 to the end of 2008.²⁹ More astoundingly, in this same time period more than 90 percent of these users had broadband access, a spike of over 100 million.³⁰ China also has the world's biggest cell phone market, with some 583.5 million subscribers.³¹ The rural-urban divide that influences many gaps in the informatization of the national economy is closing, but it remains substantial. Rural areas and the poorer western provinces are beginning to gain ground, against a national Internet penetration rate of 22.6 percent.³² At the end of 2008, rural Internet users made up almost a third of the entire online population, a jump of over 60 percent.³³ While many of the poorer and western provinces such as Yunnan, Gansu, and Guizhou continue to have penetration rates of less than 10 percent, they also have considerable growth rates, upward of 50 percent.³⁴ Driven by the policy goal that "every village has access to the telephone and every township has access to the Internet" by 2010, infrastructure development has expanded broadband Internet access to 92 percent of townships.³⁵ Gender is also an important demographic factor in the urban-rural divide, with rural male users outnumbering women by 15 percent. Internet users between the ages of 10 and 19 gained ground in 2008, increasing to 35 percent of all users and overtaking the 20–29 age group to become the leading demographic using the Internet.³⁶

Web sites registered in China are another exponential growth area, increasing by 91.4 percent since 2007.³⁷ Social media platforms continue to take hold: 210 million Internet users in China have visited video-sharing sites, 54 percent have blogs (although only 35 percent of those update them at least once every six months), almost a third participate in online discussion forums, and 19 percent belong to social networking sites.³⁸ Chinese netizens have access to a wide variety of well-developed Internet platforms for the domestic market, which have typically outpaced foreign services, such as search engines (Baidu's market share is at 63 percent compared to Google's 28 percent), online portals (the top four portals—Sohu, Sina, Tencent, and Netease—claim 73 percent of sector revenue), bulletin board services (BBS) and discussion forums, online video sites, blogs, social networking (the service Kaixin has an estimated 30 million daily users), and booming business-to-customer e-commerce.³⁹ Since 2006, when only China Netcom and China Telecom were permitted to offer pilot commercial VoIP services in selected cities,⁴⁰ the number of VoIP service providers has reached 3,000, mainly in Beijing and Shanghai, with the number of users reaching 80 million.⁴¹

In 2008, China's telecom regulator, the Ministry of Information Industry (MII), was dissolved and its functions absorbed into the new Ministry of Industry and Information Technology (MIIT).⁴² In addition to the MII mandate to regulate

telecommunications, Internet, broadband, electronics, computing, and software, the MIIT's enhanced authority includes supervision of IT development, formerly held by the National Development and Reform Commission.⁴³ Physical access to the Internet is controlled by the MIIT and is provided by eight state-licensed Internet access providers (ISPs), each of which has at least one connection to a foreign Internet backbone.⁴⁴ China's international outlet bandwidth reached 640 Gbps in 2008, an increase of 73.6 percent, but China Telecom (ChinaNET) maintained more than 50 percent of that bandwidth.⁴⁵ China Netcom (now China Unicom) joined China's second-largest ISP, China169, after China Telecom split off in 2003.⁴⁶

In an effort to boost the fixed-line phone industry's competitiveness in the mobile market, in 2008 numerous ministries jointly decided to merge the assets of the nation's six state-owned telecommunication companies and form three groups, announcing a plan to issue licenses for high-speed 3G cell phone services after the restructuring.⁴⁷ As part of the reorganization, China Netcom was fully incorporated into China Unicom in October 2008, reportedly completing the biggest merger in Chinese history.⁴⁸ In January 2009, the MIIT issued three 3G licenses, with China Unicom and China Telecom receiving licenses for established 3G services and China Mobile authorized to carry a Chinese TD-SCDMA service, so far unproven, that has been a priority of research and development for the government.⁴⁹

By sheer scope and range of topics—from online novels to video satires⁵⁰—the Internet “cannot be ignored as a battleground for spreading public opinion” and sentiment.⁵¹ Frequently, incidents that go viral (gaining widespread popularity by virtue of being shared on the Internet) are then catapulted into national prominence, frequently leading to calls for government action and response. According to Hu Yong, a journalism professor, dedicated coverage by online portals, extensive commentary on discussion forms, and the potency of Internet rumors that reverberate back into traditional media are driving convergence in the communications industry—especially in spawning “new media events” that often result in consequences for the officials, businesspeople, or celebrities involved.⁵² In an unpublished investigative report obtained by David Bandurski of the China Media Project, the vice president of People's Daily Online said that of the numerous secret internal reports sent up to the Central Party Committee each year, two-thirds of the few hundred reports given priority and action by top leaders are from the Internet Office of the State Council Information Office.⁵³

The rising prominence of collective efforts over the Internet to target and expose personal data,⁵⁴ known as “human flesh search engines,” appear to serve a voracious appetite within the Chinese online community for personal accountability. According to Xinhua, the phenomenon had its origins in 2001, when a man posted a picture of a woman he claimed to be his girlfriend on the portal Mop.com, and other Internet users identified her as a model for Microsoft, proving him a liar.⁵⁵ They can initiate

investigations as straightforward as looking for missing relatives, but sometimes stray into questionable acts of vigilantism involving threats and harassment. In the years since, the human flesh search engines have scored a series of successes in identifying corrupt officials who have acted shamefully or abused their office (and are often subsequently punished), as well as attacking private individuals engaging in perceived distasteful behavior.⁵⁶ These loosely networked efforts are capable of launching campaigns against people like Grace Wang, a Chinese student at Duke University who was filmed in April 2008 attempting to referee between two opposing groups of protesters at a "Free Tibet" action on campus.⁵⁷ After the video was posted on YouTube and other Web sites, the online reaction was swift: she was lambasted in Chinese-language discussion forums and portals for being "brainwashed" and a "race traitor," among other things, and her parents living in China went into hiding after threats were painted on their apartment.⁵⁸

At times, online activity has tested this relationship between citizens and government on a range of sensitive issues. Signed by more than 300 Chinese activists, scholars, lawyers, and others, Charter 08 was issued online on December 9, 2008, as a manifesto inspired by the founding of Charter 77 in Czechoslovakia in 1977.⁵⁹ It called for the protection of human rights, an independent judiciary, a republican system of "one person, one vote," and other comprehensive reforms.⁶⁰ Charter 08 provoked a clear response from authorities, who questioned or detained more than 100 of the original signatories, including Liu Xiaobo, a well-known dissident who was detained without process on December 8 and continued (as of May 13, 2009) to be held at an unknown location.⁶¹ However, through circulation by e-mail and other means, Charter 08 had garnered more than 7,000 signatures by early 2009.⁶²

Beyond the hot-button incidents that carry news cycles,⁶³ the interaction between top-down media supervisory structures and a more porous and unpredictable online sphere have also contributed to the rise of a number of phenomena unique to the Chinese cybersphere. The so-called *Fifty Cent Party*, a term referring to an estimated 280,000 Web commentators nationwide who zealously support the CCP and were initially rumored to net 50 cents per post, are directly organized by the government to "guide" online public opinion.⁶⁴ It had its origins at Nanjing University in 2005, where students were recruited with work-study funds to advocate the party line on an online student forum, and it has been institutionalized to the extent that the Ministry of Culture developed Web commentator trainings (complete with exams and job certification) and major Web sites are required to have in-house teams of these government-trained commentators.⁶⁵ Thus, while the government continues to aggressively intervene in news media coverage, these Fifty Cent Party members are proliferating because the CCP also has come to recognize the potential benefits of a public relations approach to online discourse.

Legal and Regulatory Frameworks

Although China's constitution formally guarantees freedom of expression and publication⁶⁶ and the protection of human rights,⁶⁷ legal and administrative regulations ensure that the Chinese Communist Party will be supported in its attempt at strict supervision of all forms of online content. The Internet has been targeted for monitoring since before it was even commercially available,⁶⁸ and the government seems intent on keeping regulatory pace with its growth and development.

Underlying all regulation of the Internet is a pantheon of proscribed content. Citizens are prohibited from disseminating between nine and eleven categories of content that appear consistently in most regulations⁶⁹; all can be considered subversive and trigger fines, content removal, and criminal liability.⁷⁰ Illegal content, although broadly and vaguely defined, provides a blueprint of topics the government considers sensitive, including endangering national security and contradicting officially accepted political theory, conducting activities in the name of an illegal civil organization, and inciting illegal assemblies or gatherings that disturb social order.⁷¹

Campaigns directed at cracking down on the perceived harmful societal effects of Internet development have been both publicly mobilized and opaquely implemented, but the latter are no less of a reality. The severity of Internet content control also fluctuates during different time periods, especially those buffering politically sensitive events. For example, an official announcement from the General Administration of Press and Publications stating that "a healthy and harmonious environment for a successful Seventeenth Party Congress" would be encouraged by stamping out "illegal news coverage" and "false news" precipitated a crackdown on political news reporting, commentary, and Internet discussion through the close of the Party Congress in October.⁷² In those sensitive months, authorities closed 18,401 "illegal" Web sites and targeted Internet data centers, the physical computers that private firms rent to offer online interactive features.⁷³

On January 5, 2009, seven ministries (including the Ministry of Public Security and the Ministry of Culture) were convened by the State Council Information Office (SCIO) to discuss selected activities for repairing the flood of "vulgar" (*disu*) content on the Internet that harms the minds and bodies of youth.⁷⁴ The crackdown was soon extended to include cell phone messages, online games and novels, videos, and radio programs; by January 23, the China Internet Illegal Information Reporting Center (CIIRC) had received nearly 19,000 reports of harmful content, leading authorities to shut down 1,250 illegal Web sites and to delete more than 3 million items.⁷⁵ The targeting of vulgar and pornographic content also netted some political casualties, notably the blog service provider Bullog.cn (*Niubo*), founded in 2006 by blogger Luo Yonghao. Bullog, which had become an important platform for liberal-leaning intellectuals and political bloggers, was shut down on January 9, 2009, for "picking up

harmful information on political and current affairs.”⁷⁶ Its closure was linked to its status as the leading domestic circulator of Charter 08,⁷⁷ as it had already survived a suspension in October 2007 during the Seventeenth Communist Party Congress and the purging of multiple high-profile blogs.⁷⁸ By April 2009, Luo had migrated the site as Bulloger.com to a server overseas, which was accessible only by proxy server and “unlikely ever to be allowed to exist in China.”⁷⁹

In addition to campaigns dedicated to “strict supervision” of online providers in order to curb various types of “harmful” information,⁸⁰ the government has managed to develop a relatively comprehensive strategy for managing online media. Since 2004, when essays and articles posted online began to be restricted more systematically, government supervision has evolved to rely largely on informal controls within official structures and stringent formal regulation. Nevertheless, it has been a challenge for the Chinese government to establish the same level of control over the Internet and online media as it has over the traditional media, because of factors including the relative decentralization of government supervision, the scale and viral possibilities of content available online, and the greater number of nonstate actors.

A major development in Chinese cyberspace since 2005 has been the flourishing of online news media, which now rank among the top online activities and reached 234 million Internet users in 2008.⁸¹ Not only do Chinese users cite the Internet as their most important source for information, more important than television and newspapers, but also the national information clearinghouse on information technology, the China Internet Network Information Center, acknowledges that “the report[ing] of major events, such as the Olympics, has enabled network[ed] media to stand on a par with mainstream media.”⁸² Supervision of the media, previously executed primarily by the Propaganda Department of the CCP, has been split with the SCIO, whose local branches have supervisory responsibility over Internet content.⁸³ As a result, most major online content providers and portals are registered in Beijing and are managed by the Beijing Internet Information Administration Bureau under the Beijing Information Office. Web sites and content providers have been reported to operate with greater or lesser levels of freedom depending on where they are registered.⁸⁴

Any organization transmitting content electronically about current politics, economic issues, and other public affairs must abide by the 2005 Provisions on the Administration of Internet News Information Services (“Internet News Regulations”).⁸⁵ These regulations introduced a complex regulatory scheme with the result that only news originating from state-supervised news outlets could be posted online. Government-licensed and authorized news agencies are limited to covering specific subjects approved by the state,⁸⁶ but at least are allowed to conduct original reporting on “current events news information,” defined as “reporting and commentary relating to politics, economics, military affairs, foreign affairs, and social and public affairs, as

well as reporting and commentary relating to fast-breaking social events.”⁸⁷ All Web sites that are nongovernmental entities, or otherwise not licensed news agencies, are restricted from performing any journalistic function, limiting them to reprinting content from central news outlets or media under the direct control of provincial governments.⁸⁸ In practice, major portals are not permitted to repost many articles published by print media online.

To discipline media, government ministries and Communist Party organs use both formal controls, such as policies and instructions and defamation liability, and informal mechanisms, including editorial responsibility for content, economic incentives, intimidation, and other forms of pressure.⁸⁹ Generally, authorities prefer to issue instructions advising on topics to be censored informally by means of short message service (SMS), chat, or e-mail, or at regular meetings with editors. Coverage of politically sensitive events is zealously managed at every stage in order to reduce the risk of exposure to the smallest possible degree.⁹⁰ This management includes prior bans on publication and time limits for obeying instructions, as well as “guidance” that serves a more propagandistic function, including instructions on whether to place news, when to place news, where to place it, and in what form it should be publicized. When “mass incidents” or major events such as the 2008 Olympic Games reach their conclusion, the grasp loosens over time, but it remains an unrelenting presence.

Despite the challenges and intense resources required to effectively police online media, many of these formal and informal controls have nevertheless been extended to Chinese cyberspace. China’s legal framework for Internet access and usage is achieved by the participation of state and nonstate actors at all institutional levels.⁹¹ Control over Internet expression and content is multilayered and achieved by distributing criminal and financial liability, licensing and registration requirements, and self-monitoring instructions to nonstate actors at every stage of access, from the ISP to the content provider and the end user. Some of these blunt and frequently applied methods include job dismissals; the closure of Web sites, often by their Web hosting service, for a broad array of infractions⁹²; and the detention of journalists, writers, and activists. In 2008, 49 individuals were known to be imprisoned for online activities,⁹³ including several (such as Huang Qi and Du Daobin) serving their second period of detention for Internet-related crimes.⁹⁴ Internet users have also been targeted for posting photographs and other multimedia online.⁹⁵ For example, journalist Qi Chonghuai was questioned by police about an article he cowrote about a corrupt local official and photographs of a luxurious government office building on the anti-corruption online forum of the Xinhua News Agency, before being sentenced to four years imprisonment on fraud and extortion charges.⁹⁶ Schoolteacher Liu Shaokun was detained on June 25, 2008, and sentenced to one year of “reeducation through labor” for posting pictures of school buildings that collapsed in the Sichuan earthquake.⁹⁷

Internet content providers, such as BBS and other user-generated sites, are directly responsible for what is published on their services.⁹⁸ All services providing Internet users with information that fail sufficiently to monitor their Web sites and report violations, or that produce, publish, or distribute harmful information, face fines and other serious consequences, including shutdown, criminal liability, and license revocation.⁹⁹ The government has used this approach to bring social media like video-sharing sites in line with the larger governing framework for Internet content regulation. The Provisions on the Management of Internet Audio and Video Programming Services (“Video Regulations”), effective January 1, 2008, were a further refinement of the government’s attempt to create a sustainable “walled garden” of self-policed local-language content for the Chinese cybersphere.¹⁰⁰ Jointly issued by the broadcast media regulator the State Administration of Radio, Film, and Television (SARFT) and the MII, the regulations require video service providers that produce their own content to obtain both a broadcast production license and rarely issued Internet news information services licenses, which are regulated by the MII,¹⁰¹ thus carrying forward the model introduced in the Internet News Regulations. Just as unlicensed service providers may not upload or transmit content for anyone, they are also prohibited from allowing any individuals to upload content pertaining to “current events” news.¹⁰²

In addition to the types of illegal content routinely proscribed in Internet regulations, SARFT issued a notice on March 30, 2009, detailing 21 unusually specific and wide-ranging additional content categories that online video providers should edit or delete.¹⁰³ These include distortions of Chinese culture and history; disparaging depictions of revolutionary leaders, heroes, police, army, or judiciary; depictions of torture; mocking depictions of catastrophe, including major natural disasters; excessively frightening images and sound effects; and “sexually suggestive or provocative content that leads to sexual thoughts.”¹⁰⁴ The notice also mandates providers to improve their content administration systems by hiring personnel to review and filter content, especially online music videos and other video entertainment, original content, and even netizen reporters (*paike*).¹⁰⁵

For the first time, individuals are singled out in the Video Regulations, so that “primary investors” and “managers” can be fined up to RMB 20,000 or barred from engaging in similar services for five years for violations such as not sufficiently policing content or changing shareholders without going through specified procedures.¹⁰⁶

Implementation of these regulations has been uneven, a trademark of many laws in China. A significant degree of uncertainty was also created by the inaugural requirement that online video service providers be either wholly state owned (as defined in Article 65 of the 2005 Company Law) or entities where the state holds the controlling interest, until the government clarified in February 2008 that this provision did not apply to already established Web sites.¹⁰⁷ Initially, 25 video-sharing portals were shut down (including 56.com), and another 32 video-sharing Web sites including

Tudou.com—China's largest video-sharing portal—were warned for hosting improper material in March 2008.¹⁰⁸ The third-largest Chinese video-sharing site, 56.com, went off-line mysteriously in June 2008 for more than a month,¹⁰⁹ and Youku.com received a license from SARFT in July 2008.¹¹⁰

Technical filtering associated with the so-called Great Firewall of China is only one tool of informal control applied in China. For example, to manage the explosion of the Chinese blogosphere, which reached 162 million blogs at the end of 2008,¹¹¹ blog service providers must not only install filters that do not allow the posting of potentially thousands of keyword combinations, but also flag certain posts for review. Comment sections, forums, and other interactive features that pose a higher risk of containing sensitive content can be shut off, while posts can be deleted or concealed by the provider so that only the author can see them.¹¹² Bloggers who are considered to have written too many troublesome posts can have their accounts canceled at will.

The unfolding of one mass incident presents a crucial case study on the range of online and media strategies to gather and communicate information, as well as government attempts to manage them. On June 22, 2008, the body of middle school student Li Shufen was found in the Ximen River in Weng'an county, Guizhou province.¹¹³ Although authorities declared her death to be caused by accidental drowning, her family believed that she was a victim of a crime and pressed for an investigation. Rumors circulated that relatives of the country party secretary and police chief were among the people Li was with on the night of her death, one of whom said she jumped suddenly while he was doing push-ups.¹¹⁴ In less than a week, the furor had grown so much that a group of hundreds of marchers heading toward government offices morphed into a crowd of up to 30,000 rioters, who surrounded a police headquarters and set fire to buildings and police vehicles.¹¹⁵ For a week, local officials were silent, and only one piece of news was released by the official Xinhua News Agency, describing protesters as "some people who did not know about the exact context of what had happened."¹¹⁶ In contrast to the silence of state-run media, numerous photos and video clips of the rioting appeared immediately on blogs and various online forums such as Tianya and the People's Daily Strong China forum, while unconfirmed and conflicting stories about the girl's death were circulated on the Internet.¹¹⁷ Angry netizens and Web site moderators dueled vigorously, with users posting in increasingly oblique and creative ways and Web sites aggressively deleting and blocking information about the incident.¹¹⁸ Furthermore, although hundreds of video clips appeared on YouTube, Chinese users could not access certain videos about the incident, and none appeared on two of biggest China's domestic video-sharing sites, Tudou.com and Uume.com.¹¹⁹ Soon after, state-run media began increasingly to report news and official announcements regarding the Weng'an riot on Chinese news sites, but without allowing Internet users to leave comments. Other media attempting to cover the story were compelled to apply for special press passes in order to secure interviews, which were

then attended by local officials.¹²⁰ By early July, state media were providing updates on the girl's cause of death and confirming that four officials had been fired as a result of the incident.¹²¹

At the same time, because these compulsory control mechanisms are actually implemented through informal processes, provider-based content control is neither narrow nor entirely predictable. A study of Chinese blog service providers demonstrated that there is substantial variation in censorship methods, the amount of content censored, and providers' transparency about deleting or depublishing content.¹²² Similar findings were reached in a Citizen Lab study of four popular search engines in China, which found significant variations in the level of transparency about filtering, actual content censored, and methods used, suggesting that there is not a comprehensive system for determining censored content.¹²³ While Google and Microsoft, which are hosted outside China, actually delisted certain search results, the two search engines hosted inside China, Yahoo and Baidu, ran their Web crawlers behind China's filtering system, and therefore did not index Web sites already blocked by the Chinese government. Although Google censored considerably less than the other search engines, it also has a practice of prioritizing authorized local content, which researcher Nart Ville-neuve found amplified the significance of the censored Web sites, as they were the only ones to offer differing viewpoints.¹²⁴ Indeed, the complexity of these informal control mechanisms was further revealed in April 2009, when an employee of China's leading search engine, Baidu, leaked a folder containing the substance and flow of internal censorship.¹²⁵ These included lists of topics, keywords, and URLs to be blocked, lists of banned forums, employee guidelines for monitoring work, censorship guidelines for the popular Baidu post bars, and guidelines of how to search for information that needed to be banned.¹²⁶

The government's filtering practices can cause considerable anger among China's Internet users, especially when entire platforms or tools such as RSS feed sites or Twitter are blocked.¹²⁷ The uses of social media form the building blocks for what blogger Isaac Mao calls sharism, where the "co-computing of people, networks, and machines" forms a networked pipeline system to spread information in the face of Internet crackdowns.¹²⁸

Because of a wide range of factors—from economic incentives and demographic factors of the online community to the dragnet of legal liability—the impact of self-censorship is likely enormous and increasingly public, if difficult to measure. Furthermore, the efforts of industry organizations at self-discipline are not entirely removed from government oversight. In promoting "Internet cooperation," officials place self-discipline hand-in-hand with admonitions to abide by Chinese laws.¹²⁹ The CIIRC encourages the reporting of "illegal" or "harmful" information and is sponsored by the Internet Society of China, formally registered as a civil society organization.¹³⁰ Yet the CIIRC cited Baidu and Google's Web and image search engines for returning a large

number of obscene and pornographic links as part of an announced official crackdown on obscene and pornographic content in January 2009. Google and Baidu were among a total of 19 Web sites singled out for harmful, vulgar content available to minors, including Sina.com, Sohu.com, Wangyi, and Tianya.¹³¹

The Chinese constitution protects people's right to criticize and make suggestions to any state organ.¹³² However, a few cases of alleged online defamation publicized in Spring 2009 exemplify how the Internet is illuminating some of the complexities of influence and power in the relationships between media, different levels of government, and citizens seeking justice.

Land requisitions for commercial development by local governments in China, where farmers are often inadequately compensated for land and suffer significant losses in income, are a common problem of poor governance and an inadequate legal system.¹³³ After petitions and other attempts to protect concerned farmers' legal rights had failed, Wu Baoquan and Wang Shuai were detained for their online criticism of local government land seizures.¹³⁴ In 2007, Wu Baoquan had posted information and conducted his own investigation about a land requisition in Ordos, Inner Mongolia, where officials forced residents off their land in order to sell it to developers, earning exorbitant profits while paying compensation well below market rates to the farmers.¹³⁵ Wu was tried twice for criminal defamation and ultimately his sentence was increased to two years, although the same court that affirmed his conviction decided to review his case in April 2009.¹³⁶

Wang Shuai was the author of a satirical blog post suggesting officials from his hometown, Lingbao city in Henan province, had misappropriated funds for combating drought by carrying out policies that actually encouraged drought in order to drive down land values and justify paying farmers less compensation for requisitioning their land.¹³⁷ He was detained in Shanghai by Lingbao officials on March 6, 2009, and released on bail only after he signed a written confession and his family agreed to cut down their fruit trees, reducing the compensation they would receive for their land.¹³⁸ As is often the case, it took media attention, this time through a story in a national newspaper, the *China Youth Daily*, to spark the online public scrutiny that would influence the outcome of Wu's case. In this instance, higher party officials issued an apology (from the Henan province chief of public security), compensated Wang for his eight days in detention, and fired the local party secretary and punished three others responsible for the unauthorized land requisition as well as demolishing crops and buildings before compensation was paid.¹³⁹

Neither Wang nor Wu was a journalist using a professional platform to disseminate information, but media were in large part responsible for exponentially expanding public awareness and discourse on their detention and the problems underpinning their cases.

The first litigation to be launched over human flesh search engines also tested how Internet libel would be dealt with under Chinese law. A Beijing woman named Jiang Yan had committed suicide in December 2007, months after learning about her husband Wang Fei's infidelity.¹⁴⁰ According to her instructions, posts from the blog diary she left recounting her ordeal were published posthumously by major Web portals, and Wang's anonymous human flesh search engine critics went to work publishing her husband's name, address, and other personal details.¹⁴¹ In March 2008, after he was publicly condemned, harassed, and fired from his job, Wang sued the classmate of his wife who had posted her blog on his Web site and the portals Daqi.com and Tianya. In December, after convening a rare panel of 54 judges, a Beijing court ruled in Wang's favor, finding that the classmate and Daqi violated Wang's rights of privacy and reputation, ordering them to pay a total of almost USD 1,200 in damages for emotional distress, remove the posts, and apologize.¹⁴² However, since Wang admitted to his infidelity, the court did not find that Wang had been slandered. It also exonerated Tianya, which had acted "appropriately" by deleting a user post containing Wang's personal information upon his request.¹⁴³ Interestingly, after issuing its judgment the Beijing district court held a press conference to recommend that the MIIT use technology to monitor Internet speech and prevent similar infringements.¹⁴⁴

While one legal scholar argued that the Chinese legal system "weighs privacy pretty heavily against free speech, even when the speech is truthful,"¹⁴⁵ the relatively low fine may not act as quite as strong a deterrent as plaintiffs like Wang may desire. However, the legal system has become increasingly responsive to those who feel victimized by the human flesh search engines, especially corrupt officials. In March 2009, the Standing Committee of the National People's Congress approved an amendment to the Criminal Law that would punish government and corporate employees with access to personal data who illegally obtain, sell, or leak such information, while Xuzhou city in Jiangsu province became the first jurisdiction to prohibit the dissemination of others' personal information on the Internet.¹⁴⁶

Surveillance

The government has continued to refine Internet surveillance mechanisms to closely track individuals' online activities.¹⁴⁷ In November 2006, the Ministry of Public Security announced the completion of the essential tasks of constructing the first stage of its "Golden Shield" project, which is a digital national surveillance network with almost complete coverage across public security units nationwide.¹⁴⁸ Despite the vagueness of public pronouncements on the implementation of the Golden Shield, the surveillance efforts of local governments, as well as organizations delegated responsibility for surveillance such as schools and ICPs, are clearly becoming more sophisticated. Since

2006, local governments have been developing “Safe City” surveillance and communications networks that connect police stations, through IP video surveillance, security cameras, and back-end data management facilities, to specific locations including Internet cafés, financial centers, and entertainment areas.¹⁴⁹ Private firms known as “censorship entrepreneurs” have also jumped into the fray, providing advanced text-mining solutions to enable censors to monitor, forecast, and “manage” online public opinion, thereby avoiding scandalous and damaging revelations such as the Internet post in June 2007 that exposed how children were kidnapped and forced into slave labor at illegal brick kilns in Shanxi province.¹⁵⁰ One company featured by international media, TRS Information Technology, claims to be the “leading search and content management technology and software provider in China,” serving over 90 percent of the State Council ministries, 50 percent of newspaper press groups, and 300 universities and colleges.¹⁵¹ Although TRS disclosed that its high-end surveillance systems had been generally adopted by police—specifically that the company had installed data-mining systems at eight Shanghai police stations so that one Internet police officer could now do the work of ten—TRS does not list the Ministry of Public Security as one of its customers.¹⁵²

Chinese law offers few viable protections for individual privacy, although clauses in most Internet laws and regulations technically provide for the confidentiality of user information. The exceptions, however, are more important. For example, regulations on the management of e-mail services provide that e-mail service providers are duty-bound to keep personal information and e-mail addresses of users confidential, and may not disclose them except with user consent or when authorized for national security reasons or criminal investigations according to procedures stipulated by law.¹⁵³ Most Internet regulations allow for disclosure of user information when required by law, for reasons involving national security, and for criminal investigations, but do not specify what formal procedures are required or what evidentiary standards must be met for the disclosure of information. In practice, as has been demonstrated in a number of cases,¹⁵⁴ all ISPs and ICPs not only must capitulate to Chinese government demands for censoring content, but also are required to assist the government in monitoring Internet users and recording their online activities. Requests to turn over personal data are often informal or provide little detail, and providers have no discretion to refuse turning over information to public security officials.¹⁵⁵

Real-Name Registration

Registration requirements are often the first step to monitoring citizens’ online activities. Although this rule is not enforced, new subscribers to ISPs have been expected to register with their local police bureaus since 1996.¹⁵⁶ In March 2005, as part of a CCP campaign to exercise tighter control over culture, education, and media, all university BBSs were ordered to block off-campus users and require users to reregister with their

personal identifying information when going online, eliminating online anonymity.¹⁵⁷ The city of Hangzhou was slated to become the first in China to require real-name Web registration for users to participate in local chat rooms or online forums, but these regulations were put on hold in May 2009.¹⁵⁸ The momentum for real-name systems might be stronger with cell phones, however. In January 2009, Beijing Mobile announced that it would begin requiring customers to show identification when purchasing its Easyown prepaid SIM cards (which amount to 70 percent of the customers on China Mobile, the nation's largest carrier) and limit purchases to three per person.¹⁵⁹

Data Retention

In China, ISPs and ICPs must fulfill data retention obligations. Internet service providers are required to record important data (such as identification, URLs visited, length of visit, and activities) about all of their users for at least 60 days and to ensure that no illegal content is being hosted on their servers.¹⁶⁰ While 78 percent of users in China connect from home, 42 percent of users also use Internet cafés as a main access location.¹⁶¹ However, since 2002, Internet cafés have been heavily regulated: all cafés are required to install filtering software, ban minors from entering, monitor the activities of their users, and record every user's identity and complete session logs for up to 60 days.¹⁶² In many cities, they are also connected by live video feed to local police stations. The providers of electronic bulletin services, including bulletin board services, online discussion forums, chat rooms, and so on, are required to monitor the contents of information released in their service system, time of release, and URL or domain name, and to keep it for 60 days.¹⁶³

Owned by Tencent, QQ is China's most popular instant messenger. This service was found to have installed a keyword-blocking program in its client software to monitor and record users' online communication, offering it to the police if required.¹⁶⁴

Filtering and surveillance are often complementary processes, especially when ISPs and ICPs that are liable for the activities of their users delegate human monitors to monitor and flag content for further review or deletion. Online communications by e-mail and instant messaging (such as QQ and Skype) are also examined and monitored by the government.¹⁶⁵ In October 2008, a joint report by the Information Warfare Monitor and ONI Asia provided a chilling example of the possibilities for surveillance conducted by nonstate actors on a massive scale.¹⁶⁶ The Chinese-marketed TOM-Skype, a version of the VoIP and chatting software Skype, kept more than a million user records in seven types of log files, including IP addresses, user names, and time and date stamps in all the log files that could be decrypted. All these log files, along with the information required to decrypt them, were kept on publicly accessible servers. For call information logs dating from August 2007, the user name and phone number of the recipient were also logged, while content filter logs dating from August

2008 also contained full texts of chat messages (which themselves contained sensitive information such as e-mail addresses, passwords, and bank card numbers). Of the eight TOM-Skype surveillance servers traced by Nart Villeneuve, one server hosted a special version designed for use in Internet cafés and contained log files and the censored keyword list, while another contained logs for TOM Online's wireless services.

The TOM-Skype surveillance system was triggered when a TOM-Skype user sent or received messages containing a banned keyword listed in a key file, and those messages were then stored in log files on a TOM-Skype server. Within the content of these messages stored in the file logs, when filtered out to eliminate English language obscenities, almost 16 percent contained the word "communist," 7 percent the word "Falun," and 2.5 percent "Taiwan independence." However, the logged messages also made reference to other content outside the range of these long-sensitive topics, such as earthquakes and milk powder.¹⁶⁷

Furthermore, the data also contained personal information of Skype users that interacted with TOM-Skype users. Users who attempt to access www.skype.com from China are redirected to skype.tom.com. While Skype claimed that TOM fixed the security breaches within 24 hours of the report's publication,¹⁶⁸ the report issued a warning for "groups engaging in political activism or promoting the use of censorship circumvention technology accessed through services provided by companies that have compromised on human rights." From the information contained in the log files, it would be possible to conduct politically motivated surveillance by using simple social networking tools to identify the relationships between users.

Like all other ICPs, most bulletin boards and chat rooms assign personnel to monitor the content of messages.¹⁶⁹ Messages submitted by users are censored by human censors and filtering systems before appearing online.¹⁷⁰ In order to enhance the surveillance on bulletin board systems, since 2005 the users of campus bulletin boards have been mandated to reregister with their real identifying information before posting messages online.¹⁷¹

In recent years, serious concerns have been raised about the ability of the Chinese government to spy on the country's 624 million cell phone subscribers: in 2008, one Chinese state-run cell phone company revealed that it had unlimited access to the personal data of their customers and hands the data over to Chinese security officials upon request.¹⁷² Since 2004, the Chinese government has been drafting legislation to regulate personal mobile phone communication, which would require all cell phone subscribers to register for mobile phone service with their real name and identification card.¹⁷³ In addition, Chinese police have installed filtering and surveillance systems for mobile and SMS providers to block and monitor "harmful" short-message communications.¹⁷⁴ Anyone who distributes "harmful" messages or rumors using SMS on mobile phones can be arrested and convicted.¹⁷⁵

Cyber Attacks

In 2008, organizations advocating for human rights in Tibet and China experienced escalated cyber attacks during politically explosive events, such as the crackdown on Tibetan protesters in March, and in the lead-up to the Olympic Games in August. The preferred method of these attackers was reportedly e-mail viruses, which are more likely to be undetected by commercial antivirus software because they are hand-crafted.¹⁷⁶ From field research conducted at the offices of the Tibetan Government in exile in Dharamsala and several Tibetan missions abroad, researchers at the SecDev Group and the Citizen Lab at the University of Toronto discovered an extensive malware-based cyber-espionage network that also used “contextually relevant e-mails” to gain “complete, real-time” control of at least 1,295 infected computers in 103 countries.¹⁷⁷ This network, which they called GhostNet, sent e-mails to specific targets containing a Trojan called Gh0st RAT, which in taking full control of infected computers allowed GhostNet to search and download specific files and covertly operate attached devices such as microphones and Web cameras. Among the high-value infections, comprising close to 30 percent of the computers affected, were many foreign affairs ministries, embassies, regional organizations (such as the ASEAN Secretariat), and news organizations. Although the complicity or awareness of Chinese authorities could not be conclusively established, researchers tracked the instances of Gh0st RAT to commercial Internet access accounts located on the island of Hainan in China.

ONI Testing Results

The “Great Firewall of China” uses a variety of overlapping techniques for blocking content containing a wide range of material considered politically sensitive by the Chinese government. While China employs filtering techniques used by many other countries, including domain name system (DNS) tampering and Internet protocol (IP) blocking, it is unique in the world for its system of filtration, targeting Internet connections when triggered by a list of banned keywords. Known as a TCP reset, this content filtering by keyword targets content regardless of where it is hosted.

Reset filtering using TCP is based on inspecting the content of IP packets for keywords that would trigger blocking, either in the header or the content of the message. When a router in the Great Firewall identifies a bad keyword, it sends reset packets to both the source and destination IP addresses in the packet, breaking the connection.

China employs targeted yet extensive filtering of information that could have a potential impact on the Communist Party’s control over social stability, and is therefore predominantly focused on Chinese-language content relating to China-specific issues. For the government, information constituting a threat to public order extends well beyond well-publicized sensitive topics, such as the June 1989 military crackdown,

the Tibetan rights movement, and the Falun Gong spiritual organization (all of which are methodically blocked), and includes independent media and dissenting voices, as well as content on human rights, political reform, sovereignty issues, and circumvention tools.

Filtering during the 2008 Olympic Games

The OpenNet Initiative monitored a short list of prominent blogs, Chinese-language and international news sites, advocacy organizations, and social media platforms continuously from late July to mid-September 2008. This period generally marked one of the most significant openings in access to information since ONI began monitoring Internet filtering in China in 2004, but the foundations of censorship based on control over domestic media and civil society remained.

In 2001, China issued this decree in its official bid for the 2008 Olympic Games: “There will be no restrictions on journalists in reporting on the Olympic Games.”¹⁷⁸ This promise was significantly compromised, not only in China’s purported long-term attempt to build a more open and transparent media system,¹⁷⁹ but also in the lack of transparency over its policy on access to online information.

At a press conference on July 28, the media director of the Beijing Olympic Committee responded to a *Wall Street Journal* reporter who physically displayed the filtering of certain Web sites on his laptop by denying anything was amiss.¹⁸⁰ This time, a Chinese Foreign Ministry spokesperson laid part of the blame with the Web sites themselves, claiming they have problems making them “not easy to view in China.”¹⁸¹ Yet, three days later, on July 31, the IOC admitted to accepting a deal with the Chinese government in which sensitive Web sites that were “not considered Games-related” would be blocked.¹⁸²

During the Olympics, access was partitioned between the Olympics Main Press Center (MPC) in the Olympic Green and the Beijing International Media Center, the main press venue for non-IOC-accredited journalists.¹⁸³ The ONI compared data from the Olympics MPC to that from other locations in Beijing, compiling a snapshot of Internet filtering in China leading up to the Olympics. Testing conducted by the ONI at the Olympics MPC confirmed that filtering of Internet content continued even for members of the foreign press through TCP reset keyword blocking and IP address blocking, the latter accounting for the vast majority of filtering at the MPC. For each test at the MPC, the ONI tested at other locations in Beijing with broadband Internet access provided by China Netcom. Throughout this time period, filtering was nearly identical between the MPC and consumer-level access on China Netcom and China Telecom, indicating that the incrementally increased openness was implemented nationally.

Many sites that are routinely blocked by the Chinese government for containing politically sensitive content remained accessible from August 1 to at least mid-September 2008, including the Web sites of human rights organizations and foreign-hosted

Chinese-language news sites. Overseas news organizations such as the World Journal and the BBC News Chinese Web site were the main beneficiaries of China's Olympic guarantees.

Even though the IOC acknowledged on July 31 that filtering would continue to take place, a number of Web sites blocked at the MPC on July 25 were accessible a week later, including Amnesty International, Chinese-language Wikipedia (zh.wikipedia.org), and an increased swath of independent media including Taiwan's *Liberty Times*, the Hong Kong-based *Apple Daily* newspaper, Voice of America news, and Radio Free Asia (www.rfa.org) and its Chinese Web site.

However, RFA's Tibetan- and Uyghur-language Web sites became inaccessible again around August 20. Although Flickr remained accessible throughout the testing period, two of its photo servers were filtered until mid-August. Most of the sites unblocked for the Olympics remained accessible until at least mid-September 2008 on China Netcom, although a few (including Amnesty International) were again blocked on China Telecom by September 15.

At the same time, the ONI found that the sites being filtered frequently address tumultuous and controversial changes wrought in preparation for the games, from crackdowns on civil society to the transformation of a capital city and other social upheavals. Thus, the majority of advocacy sites and politically "sensitive" organizations remained blocked, sweeping across a broad range of issues from citizen journalism (www.zuola.com) to the Three Gorges Probe, as well as nearly all of the Tibetan exile advocacy groups. Groups staunchly critical of Chinese government policy, including the press freedom groups Reporters Without Borders and Freedom House, continued to be blocked. The status of certain news sites, including the China Digital Times Internet news and information clearinghouse and Boxun.com, a dissident news Web site that Chinese government officials reportedly look to as a source of internal news, remained unchanged. Furthermore, the accessibility of any Web site does not guarantee that content on that site will be available, as China's practice of filtering keywords through a TCP reset appears as robust as ever.

On December 19, 2008, the Web site of the *New York Times* was reported blocked even as restrictions were lifted on the Chinese-language Web sites of the BBC, Voice of America, and Asiaweek, which had been blocked earlier that week.¹⁸⁴

In addition to testing during the Olympics period, the ONI also conducted testing in late 2008 on two backbone providers, the state-owned telecoms China Unicom (CU), formerly China Netcom, and China Telecom (CT), which between them provide coverage nationwide. Because both control access to an international gateway, URL filtering and domain name system (DNS) tampering implemented by CU and CT affect all users of the network regardless of ISP.

Nearly all the DNS tampering was executed by CU, while CT blocked a number of human rights organizations, pornographic sites, and one Hong Kong-based publisher

(mirrorbooks.com) using this method. China Unicom also used IP blocking to filter nearly 400 IP addresses. These correlated closely with sites blocked on CT through a method obscured to analysis, in which users were presented with an error page informing the user that a network error occurred while accessing the Web site. While the error page can appear in the case of legitimate network errors, the repeated appearance of the error page indicates blocking is taking place. China Telecom also used a squid proxy to block a handful of Web sites, including several Flickr photo servers. While the two backbone providers showed less overlap in filtering methods when compared with 2006–2007, there continued to be almost complete correlation in blocking between CU and CT.

At time of testing, most international social media platforms were accessible, including Flickr, Blogspot, Wordpress, Facebook, and Twitter. In contrast to 2006–2007, when all individual Blogspot blogs tested were accessible on China Netcom and blocked or inaccessible on China Telecom, in 2008 CU and CT blocked nearly all of the same individual Blogspot blogs tested. Technorati continued to be blocked.

In late 2008, China had resumed blocking many Web sites that were blocked in 2006–2007 and made accessible during at least part of the Olympics period. These included the independent overseas news sites (*The Liberty Times*) and Radio Free Asia's main Web site and its Mandarin-, Uyghur-, and Tibetan-language sites. However, in contrast to 2006–2007, some of these Web sites were unreliably or intermittently accessible during December 2008 testing, possibly as a result of the TCP reset filtering method used. Sites blocked using the TCP reset included YouTube, Chinese-language Wikipedia, and BBC News.

A few sites that were accessible in 2006–2007 had been blocked by 2008 testing, most notably Wikipedia (en.wikipedia.org). The site Wikileaks (www.wikileaks.org) was also blocked by both ISPs in 2008 testing.

The greatest variations in filtering patterns between 2006–2007 and 2008 occurred with Chinese-language news media Web sites, likely in continuity from the Olympics. As in 2006–2007, few international news organizations were filtered, and some formerly blocked (e.g., Voice of America news) were accessible. Notably, some prominent Chinese-language media blocked in 2006–2007 were accessible in 2008, including the World Journal, www.singtao.com, and the *Apple Daily*. However, a significant number of independent media representing different points on the political spectrum continued to be filtered.

In 2006–2007 and 2008, China filtered a significant portion of content specific to its own human rights record and practices. As such, only a few global human rights sites with a global scope continued to be filtered, including Human Rights and Freedom House. Article 19 and Human Rights First were no longer blocked in 2008, and filtering on Amnesty International was renewed after a hiatus during the Olympics period. A typical example of this targeting of China-related content is the differential treatment

of two related organizations: while the Web site for the writers' association PEN American Center hosted content on the jailed dissident and Charter 08 coauthor Liu Xiaobo, it was accessible (www.pen.org) at the same time that the Chinese PEN Center (www.chinesepen.org), a site with both English and Chinese content, was blocked by both ISPs. The sites of watchdogs on Chinese rights defenders and labor rights continued to be blocked, as did a substantial number of rights organizations based in Hong Kong.

Certain targets for blocking continued to cut across political and social lines of conflict in 2008. The consistent filtering of Web sites supporting greater autonomy and rights protection for the Uyghur (www.uyghurcongress.org), Tibetan, and Mongolian (www.innermongolia.org) ethnic minorities is not surprising, as these issues have already been excluded from official discourse inside China. Nearly all the overseas Tibetan organizations, which conduct activities ranging from news broadcasting for the Tibetan community to the Tibetan Youth Congress, which lobbies for full independence for Tibet, have been blocked. China also continued to block a substantial number of sites on religion, including the International Coalition for Religious Freedom, Catholic organizations, and sites on Islam in Arabic, including those presenting extremist viewpoints (www.alumah.com).

In 2008, China continued to filter a significant number of sites presenting alternative or additional perspectives on its policies toward Taiwan and North Korea. For example, the Democratic Progressive Party (DPP) of Taiwan (www.dpp.org.tw) is continually filtered. However, a number of sites with no political content but ending with the domain ".tw" were blocked, and Greenpeace Taiwan was the only country Web site of the organization blocked by both ISPs.

As in 2006–2007, the major exceptions to the focus on politically sensitive topics specific to China in 2008 were circumvention tools and pornography. A portion, though not a majority, of proxy tools and anonymizers in both the Chinese (garden-networks.com) and English (www.peacefire.org) languages were blocked. The circumvention tool Psiphon was also blocked, along with the Web sites of the Citizen Lab at the University of Toronto and the Information Warfare Monitor, sister institutions engaging in research on circumvention and surveillance. Both ISPs also blocked a substantial amount of pornographic content.

Although the scope of Internet filtering in China extends far beyond the highly sensitive issues known as the "three Ts: Tibet, Tiananmen, and Taiwan," the continued potency of these subjects evidently prompted the Chinese government to step up filtering of leading international Web sites and social media platforms in 2009. On March 24, 2009, Google officially confirmed that YouTube was blocked in China; traffic dropped steeply on the evening of March 23 to "near zero" by March 24.¹⁸⁵ The Web site www.herdict.org also captured accounts providing evidence of a previous reported

block of YouTube beginning on March 4, coinciding with the one-year anniversary of the crackdown on protests in Tibetan regions (during which YouTube was also reported blocked in March 2008) as well as the 50th anniversary of the Tibetan uprising of 1959. Blogspot became inaccessible around May 9,¹⁸⁶ and on June 2, two days before the 20th anniversary of the June 4 military crackdown, Flickr, Twitter, live.com, and Hotmail were blocked in rapid succession.¹⁸⁷

In May 2009, the Ministry of Industry and Information Technology in China sent a notification to computer manufacturers of its intention to require all new PCs sold in China after July 1 to have filtering software preinstalled.¹⁸⁸ The notice, jointly issued by the MIIT, the Civilization Office of the Central Communist Party Committee, and the Ministry of Finance, according to the PRC Government Procurement Law, mandates the procurement of all rights and services related to a designated software called “Green Dam Youth Escort” to be made available for free public use. Green Dam is a product of the Jinhui Computer System Engineering Company, which reportedly received RMB 40 million from the government for a year-long contract.¹⁸⁹

The purported intent of the Green Dam software is to filter harmful online text and image content in order to prevent this information from affecting youth and promote a healthy and harmonious Internet environment.¹⁹⁰ However, researchers at the OpenNet Initiative and the Stop Badware Project conducting an initial technical assessment of the software found that Green Dam’s filtering not only is ineffective at blocking pornographic content as a whole, but also includes unpredictable and disruptive blocking of political and religious content normally associated with the Great Firewall of China.¹⁹¹

As a computing tool, Green Dam is far more powerful than the centralized filtering system China currently implements, as it actively monitors individual computer behavior to the extent that its “language processing” tool can institute extremely intrusive “kill” action on sites if the content algorithm detects “inappropriate” sensitive political or religious speech.¹⁹² These actions include the sudden termination of Web browser tabs, whole browsers, and a wide range of programs including word processing and e-mail. The program installs components deep into the kernel of the computer operating system in order to enable this application layer monitoring. Researchers also found that the killing of sites upon inappropriate keywords or URLs like <http://falundafa.org> extends to killing single letters that autocomplete in location boxes and autocomplete lists in browsers. For example, if a user enters “epochtimes.com” into the location, the user will see the page briefly, see the warning box briefly, and then have the whole browser terminated. But after the user restarts the browser, epochtimes.com will be in the browser history and therefore in the autocomplete list, so that the user may only have to type “e” into the location box to trigger the appearance of epochtimes.com in the autocomplete list and cause Green Dam to terminate the whole browser.¹⁹³

The monopoly status granted to Jinhui is unprecedented, representing the first instance where a government mandated a specific filtering software product for use at a national level instead of performance standards that encourage consumer choice, security, and product quality. The mandated procurement and preinstallation of Green Dam also adds a new and powerful control mechanism to the existing filtering system, in addition to blocking already done at the international backbones and by individual online content providers. Distributing control mechanisms to end users at the periphery allows the government to partially offload the burden of monitoring and blocking content to individual machines on the network, amounting to a “huge distributed super computer dedicated to controlling online content.”¹⁹⁴

In addition to interfering with the performance of personal computers in an unpredictable way, the poor design of Green Dam also presents security risks that allow any Web site the user visits to take control of the user’s computer, with the potential for malicious sites to steal private data and commit other illegal acts, or even turn every Chinese computer running Green Dam into a member of a botnet.¹⁹⁵ The Stop Badware Project at the Berkman Center for Internet and Society confirmed that the application violates its Badware guidelines for software, as it does not disclose the filtering of political speech or the unexpected behavior of completely killing processes that contain such speech.¹⁹⁶

Conclusion

The Chinese government has maintained a strict and vigorous approach toward Internet censorship, interfering with public knowledge and discourse through pervasive filtering practices and a multitude of nontechnical methods. In 2008, China led the world with 300 million Internet users, and the sheer scale and expanding scope of online content presented a significant challenge for a government intent on maintaining social stability and order in China’s networked spheres. China continues to fine-tune its system of information control, including attempts to promote a public relations approach to online commentary and news reporting. The foundation of China’s information-control framework continues to be built on ensuring that domestic providers are responsible for filtering and monitoring hosted content. The government has also taken measures to distribute control mechanisms to end users through the procurement of filtering software on home computers. The 2008 Olympic Games held in Beijing had a net positive impact on access to information, but this has abated without continued international pressure for greater openness and transparency.

Notes

1. Jim Yardley, “Monk Protests in Tibet Draw Chinese Security,” *New York Times*, March 14, 2008, <http://www.nytimes.com/2008/03/14/world/asia/14china.html>.

2. Jim Yardley, "Tibetans Clash with Chinese Police in Second City," *New York Times*, March 16, 2008, <http://www.nytimes.com/2008/03/16/world/asia/16tibet.html?ref=asia>.
3. Roland Soong, "The Olympic Torch Tour as Public Relations Disaster," EastSouthWestNorth blog, April 10, 2008, http://zoniaeuropa.com/20080410_1.htm.
4. Dune Lawrence and Lee Spears, "China Rejects CNN Apology, Demands 'Sincere' Response," Bloomberg, April 17, 2008, <http://www.bloomberg.com/apps/news?pid=20601204&sid=aVifJJeTKWMC>; Xinhua News Agency, "Chinese Netizens Urge Carrefour Boycott after Torch Relay Incident," April 16, 2008, http://news.xinhuanet.com/english/2008-04/16/content_7989807.htm.
5. *BBC News*, "China Earthquake Toll Jumps Again," May 23, 2008, <http://news.bbc.co.uk/2/hi/asia-pacific/7416035.stm>.
6. Qian Gang, "Looking Back on Chinese Media Reporting of School Collapses," China Media Project, May 7, 2009, <http://cmp.hku.hk/2009/05/07/1599/>; Edward Wong, "Year after China Quake, New Births, Old Wounds," *New York Times*, May 6, 2009, <http://www.nytimes.com/2009/05/06/world/asia/06quake.html>.
7. Tania Branigan, "China Releases Earthquake Death Toll of Children," *Guardian*, May 7, 2009, <http://www.guardian.co.uk/world/2009/may/07/china-earthquake-anniversary-death-toll>.
8. Qian Gang, "Looking Back on Chinese Media Reporting of School Collapses," China Media Project, May 7, 2009, <http://cmp.hku.hk/2009/05/07/1599/>.
9. Michael Bristow, "Big Olympic Spend, but Little Debate," *BBC News*, July 31, 2008, <http://news.bbc.co.uk/2/hi/asia-pacific/7523235.stm>.
10. Xinhua News Agency, "Regulations on Reporting Activities in China by Foreign Journalists during the Beijing Olympic Games and the Preparatory Period," January 8, 2007, <http://www.chinese-embassy.org.uk/eng/lsw/Journalist/t287657.htm>.
11. Jacquelin Magnay, "China's Media Censored over Stabbing," *The Age*, August 12, 2008, <http://www.theage.com.au/world/chinas-media-censored-over-stabbing-20080811-3tmf.html>.
12. OpenNet Initiative Blog, "The Catch-22 of Protests and Surveillance," August 19, 2008, <http://opennet.net/blog/2008/08/the-catch-22-protests-and-surveillance>.
13. Foreign Correspondents' Club of China, "Reporting Interference Tally Update," December 3, 2008, <http://www.fccchina.org/2008/12/03/reporting-interference-tally-update/>; Foreign Correspondents' Club of China, "China Fails to Make Olympic Podium on Media Freedom," August 23, 2008, <http://www.fccchina.org/2008/08/23/china-fails-to-make-olympic-podium-on-media-freedom/#more-35>.
14. *BBC News*, "China's Press Freedoms Extended," October 18, 2008, <http://news.bbc.co.uk/2/hi/asia-pacific/7675306.stm>.
15. Foreign Correspondents' Club of China, "FCCC Urges Withdrawal of Restrictions on HK Journalists," February 13, 2009, <http://www.fccchina.org/2009/02/13/fccc-urges-withdrawal-of-restrictions-on-hk-journalists/>.

16. Xinhua News Agency, "60 Arrested over Melamine-Tainted Sanlu Milk Powder," January 11, 2009, http://www2.chinadaily.com.cn/china/2009-01/11/content_7385532.htm.
17. *The Australian*, "China Accused of Olympic Milk Cover-up," October 1, 2008, <http://www.theaustralian.news.com.au/story/0,25197,24430439-2703,00.html>.
18. Jim Yardley and David Barboza, "Despite Warnings, China's Regulators Failed to Stop Tainted Milk," *New York Times*, September 27, 2008, <http://www.nytimes.com/2008/09/27/world/asia/27milk.html?pagewanted=print>.
19. Ibid.
20. Zhu Zhe and Cui Xiaohuo, "Sanlu Ex-Boss Gets Life for Milk Scandal," *China Daily*, January 22, 2009, http://www.chinadaily.com.cn/china/2009-01/22/content_7422297.htm.
21. David Bandurski, "Taxi Strikes in China Highlight Changing Press Controls," China Media Project, November 12, 2008, <http://cmp.hku.hk/2008/11/12/1344/>.
22. Tania Branigan, "China Tells State Media to Report Bad News," *Guardian*, November 20, 2008, <http://www.guardian.co.uk/media/2008/nov/20/china-media-freedom>.
23. Maureen Fan, "In China, Media Make Small Strides," *Washington Post*, December 28, 2008, <http://www.washingtonpost.com/wp-dyn/content/article/2008/12/27/AR2008122701218.html>.
24. David Bandurski, "The Longnan Riots and the CCP's Global Spin Campaign," China Media Project, November 20, 2008, <http://cmp.hku.hk/2008/11/20/1368/>.
25. Reuters, "China to Introduce Journalist 'Black List,'" February 13, 2009, <http://in.reuters.com/article/worldNews/idINIndia-37996920090213?sp=true>.
26. David Bandurski, "In Today's Headlines, an Absence Speaks a Thousand Words," China Media Project, May 27, 2009, <http://cmp.hku.hk/2009/05/27/1647/>.
27. Andrew Jacobs and Jonathan Ansfield, "Chinese Learn Limits of Online Freedom as the Filter Tightens," *New York Times*, February 5, 2009, <http://www.nytimes.com/2009/02/05/world/asia/05beijing.html>.
28. Foreign Correspondents' Club of China, "China Should Allow Access to Tibetan Areas," March 9, 2009, <http://www.fccchina.org/2009/03/09/china-should-allow-access-to-tibetan-areas/>.
29. China Internet Network Information Center, "Statistical Survey Report on the Internet Development in China," March 23, 2009, <http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf>.
30. Ibid.
31. Janet Ong, "China to Merge Telecom Companies, Issue 3G Licenses," Bloomberg, May 24, 2008, http://www.bloomberg.com/apps/news?pid=20601087&sid=an0_Sig7jjE0&refer=home.
32. China Internet Network Information Center, "Statistical Survey Report on the Internet Development in China," March 23, 2009, <http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf>.

33. Ibid.

34. Ibid.

35. Zhao Zhiguo, "Development and Administration of the Internet in China," China.org.cn, November 7, 2008, http://www.china.org.cn/china/internetForum/2008-11/06/content_16719106.htm.

36. China Internet Network Information Center, "Statistical Survey Report on the Internet Development in China," March 23, 2009, <http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf>.

37. Ibid.

38. Ibid.

39. Paul Budde Communication Pty., Ltd., "China—New Internet Economy," April 24, 2009.

40. SinoCast China IT Watch, "China to Issue Its First VoIP License," March 13, 2006.

41. CC Time, "Analysis of Recent Developments and Forecasts for China's VOIP Industry," March 19, 2008, <http://www.cctime.com/html/2008-3-19/20083191040597146.htm>.

42. See Ministry of Industry and Information Technology of the People's Republic of China, <http://www.miit.gov.cn/n11293472/index.html>.

43. *People's Daily Online*, "Highlights of China's Institutional Restructuring Plan," March 16, 2008, <http://english.peopledaily.com.cn/90001/90776/90785/6374104.html>.

44. China Internet Network Information Center, "Statistical Survey Report on the Internet Development in China," March 23, 2009, <http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf>.

45. Ibid.

46. Paul Budde Communication Pty., Ltd., "China—Telecommunications Infrastructure," April 24, 2009.

47. Ibid.

48. Xinhua News Agency, "China Netcom, China Unicom Merger Completed, Biggest in Country's History," October 15, 2008, http://news.xinhuanet.com/english/2008-10/15/content_10200183.htm.

49. Sumner Lemon, "After Years of Delays, China Finally Issues 3G Licenses," *PCWorld*, January 7, 2009, http://www.pcworld.com/businesscenter/article/156612/after_years_of_delays_china_finally_issues_3g_licenses.html.

50. "Nnali you hexie, nali you caonima," or, "Where there are river crabs, there are grass-mud horses," is based on plays on characters and meaning, forming a "law of Chinese cyberpolitics": online censorship always meets resistance. See China Digital Times, "Grass Mud Horse," <http://chinadigitaltimes.net/china/grass-mud-horse/>.

51. China Internet Network Information Center, "Statistical Survey Report on the Internet Development in China," March 23, 2009, <http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf>.
52. Alice Xin Liu, "Hu Yong Interview: The Digital Age, Orwell's 'Newspeak' and Chinese Media," Danwei, April 16, 2009, http://www.danwei.org/media/hu_yong_interview.php.
53. David Bandurski, "China's Guerrilla War for the Web," *Far Eastern Economic Review*, July 2008, <http://www.feer.com/essays/2008/august/chinas-guerrilla-war-for-the-web>.
54. Dave Lyons, "Day 2 4.1: Chen Lu, Human Flesh Search," Global Voices, One World blog, May 28, 2009, <http://www.lokman.org/2009/05/28/day-2-41-chen-lu-human-flesh-search/>.
55. Bai Xu and Ji Shaoting, "'Human Flesh Search Engine': An Internet Lynching?" Xinhua News Service, July 4, 2008, http://news.xinhuanet.com/english/2008-07/04/content_8491087.htm.
56. Ryan McLaughlin, "Human Flesh Search Engines—Crowd-Sourcing 'Justice'," CNet Asia Blogs, January 28, 2009, <http://asia.cnet.com/blogs/thetechdynasty/post.htm?id=63008617>.
57. The video footage is available on YouTube, <http://www.youtube.com/watch?v=zomgZuZoDoM>.
58. National Public Radio, "Duke Student Targeted for Mediating Tibet Protest," April 21, 2008, <http://www.npr.org/templates/story/story.php?storyId=89803198>.
59. *New York Review of Books*, "China's Charter 08" [unofficial translation by Perry Link], January 15, 2009, <http://www.nybooks.com/articles/22210>.
60. Ibid.
61. China Human Rights Defenders, "Over One Hundred Signatories Harassed since Launch of Charter 08," January 8, 2009, http://crd-net.org/Article/Class9/Class98/200901/20090108141140_12945.html.
62. John Garnaut, "Late-Night Visit from Police as Charter 08 Support Grows," *Sydney Morning Herald*, January 13, 2009, <http://www.smh.com.au/articles/2009/01/12/1231608616941.html>.
63. Roland Soong, "A Review of the Chinese Internet in 2008," EastSouthWestNorth blog, January 24, 2009, http://www.zonaeuropa.com/20090124_1.htm.
64. David Bandurski, "China's Guerrilla War for the Web," *Far Eastern Economic Review*, July 2008, <http://www.feer.com/essays/2008/august/chinas-guerrilla-war-for-the-web>.
65. Ibid.
66. Article 34, Constitution of the People's Republic of China, amended March 14, 2004, by the 10th NPC at its 2nd Session, <http://english.peopledaily.com.cn/constitution/constitution.html>.
67. Ibid.
68. See State Council, *Zhonghua Renmin Gongheguo Jisuanji Xitong Anquan Baohu Tiaoli* [The Regulations of the People's Republic of China for the Safety Protection of Computer Information Systems], February 18, 1994.

69. The nine types of content that have been illegal to produce or disseminate since the earliest Internet Regulations are (1) violating the basic principles as they are confirmed in the Constitution; (2) endangering state security, divulging state secrets, subverting the national regime, or jeopardizing the integrity of national unity; (3) harming national honor or interests; (4) inciting hatred against peoples, racism against peoples, or disrupting the solidarity of peoples; (5) disrupting national policies on religion, propagating evil cults and feudal superstitions; (6) spreading rumors, disturbing social order, or disrupting social stability; (7) spreading obscenity, pornography, gambling, violence, or terror, or abetting the commission of a crime; (8) insulting or defaming third parties, infringing on legal rights and interests of third parties; and (9) other content prohibited by law and administrative regulations. Two categories of prohibited content were added in Article 19 of the Provisions on the Administration of Internet News Information Services (Internet News Information Services Regulations) (*hulianwang xinwen xinxi fuwu guanli guiding*), promulgated by the State Council Information Office and the Ministry of Information Industry on September 25, 2005. These two additional categories are (1) inciting illegal assemblies, associations, marches, demonstrations, or gatherings that disturb social order; and (2) conducting activities in the name of an illegal civil organization. Unofficial English translation is available at Congressional Executive Commission on China Virtual Academy, "Provisions on the Administration of Internet News Information Services," September 25, 2005, <http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396>.

70. See NPC Standing Committee, *Quanguo renda changweihui guanyu wei hu hulianwang anquan de guiding* [Rules of the NPC standing committee on safeguarding Internet security], December 28, 2000.

71. Ministry of Information Industry and the State Council Information Office, *hulianwang xinwen xinxi fuwu guanli guiding* [Provisions on the administration of news information services], September 25, 2005, <http://www.isc.org.cn/20020417/ca315779.htm>; Congressional Executive Commission on China Virtual Academy, "Provisions on the Administration of Internet News Information Services."

72. Human Rights Watch, "China: Media Chokehold Tightens before Party Congress," August 17, 2007, http://china.hrw.org/press/news_release/china_media_chokehold_tightens_before_party_congress; Michael Bristow, "China Tightens Grip Ahead of Congress," BBC News, September 14, 2007, <http://news.bbc.co.uk/2/hi/asia-pacific/6992946.stm>.

73. Peter Ford, "Why China Shut Down 18,401 Websites," *Christian Science Monitor*, September 25, 2007, <http://www.csmonitor.com/2007/0925/p01s06-woap.html?page=1>.

74. Xinhua News Agency, "*qi bumen kaizhan zhengzhi hulianwang disu zhifeng xingdong*" [Seven departments launch operation for fixing the spread of vulgarity on the Internet], January 5, 2009, http://www.gov.cn/jrzg/2009-01/05/content_1196447.htm.

75. Xinhua News Agency, "Porn Crackdown to Shield China's Youth during Holiday," *China.org.cn*, January 23, 2008, http://www.china.org.cn/china/news/2009-01/23/content_17178010.htm.

76. Vivian Wu, "Popular Blog Service Provider Shut Down," *South China Morning Post*, January 10, 2009.

77. John Garnaut, "Nervous China Tightens Grip on Internet," *Sydney Morning Herald*, January 12, 2009.

78. *China Digital Times*, "Bullog Shut Down," January 9, 2009, <http://chinadigitaltimes.net/2009/01/bullog-shut-down/>.

79. Radio Free Asia, "China Closes 'Porn' Sites," April 1, 2009, <http://www.rfa.org/english/news/china/internet-04012009101155.html>.

80. For example, in June 2006, the Information Office under the State Council and the MII embarked on a period of "strict supervision" of search engines, chat rooms, and blog service providers to curb the circulation of "harmful" information online. See Howard W. French, "Chinese Discuss Plan to Tighten Restrictions on Cyberspace," *New York Times*, July 4, 2006, <http://www.nytimes.com/2006/07/04/world/asia/04internet.html>.

81. China Internet Network Information Center, "Statistical Survey Report on the Internet Development in China," March 23, 2009, <http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf>.

82. *Ibid.*

83. David Shambaugh, "China's Propaganda System: Institutions, Processes, and Efficacy," *China Journal*, No. 57 (January 2007): 25–58.

84. Rebecca MacKinnon, "China's Censorship 2.0: How Companies Censor Bloggers," *First Monday*, 14, No. 2 (2009), <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089>.

85. Ministry of Information Industry and the State Council Information Office, *hulianwang xinwen xinxi fuwu guanli guiding* [Provisions on the administration of news information services], September 25, 2005, <http://www.isc.org.cn/20020417/ca315779.htm>; Congressional Executive Commission on China Virtual Academy, "Provisions on the Administration of Internet News Information Services."

86. *Ibid.*

87. *Ibid.*

88. *Ibid.*

89. Benjamin Liebman, "Watchdog or Demagogue? The Media in the Chinese Legal System," *Columbia Law Review*, 105, No. 1 (January 2005): 41.

90. Stephanie Wang and Robert Faris, "Welcome to the Machine," *Index on Censorship*, 37, No. 2, (May 2008): 106–113.

91. Anne S.Y. Cheung, "The Business of Governance: China's Legislation on Content Regulation in Cyberspace," *New York University Journal of International Law and Politics*, 28 (Fall 2005–Winter 2006): 1–37

92. Chinese Human Rights Defenders, "Tug of War over China's Cyberspace: A Sequel to Journey to the Heart of Censorship (Part II)," March 19, 2009, http://crd-net.org/Article/Class9/Class11/200903/20090319000543_14370.html.
93. Reporters Without Borders, "2009 Annual Report: China," <http://www.rsf.org/en-rapport57-China.html>.
94. Chinese Human Rights Defenders, "Tug of War over China's Cyberspace: A Sequel to Journey to the Heart of Censorship (Part II)," March 19, 2009, http://crd-net.org/Article/Class9/Class11/200903/20090319000543_14370.html.
95. Chinese Human Rights Defenders, "*Zhongguo Wangluo Jiankong Yu Fanjiankong Niandu Baogao*" [Annual Report on Chinese Internet Surveillance 2007], July 10, 2008, http://www.crd-net.org/Article/Class1/200807/20080710165332_9340.html.
96. Reporters Without Borders, "Journalist Gets Four Years for Exposing Communist Party Corruption in Shandong," May 15, 2008, http://www.rsf.org/article.php3?id_article=27034.
97. Human Rights in China, "Family Visits Still Denied to Sichuan School Teacher Punished after Quake-Zone Visit," July 29, 2008, http://www.hrichina.org/public/contents/press?revision_id=66556&item_id=66524.
98. Ministry of Information Industry, Article 13, *Hulianwang dianzi gonggao fuwu guanli guiding* [Rules on the management of Internet electronic bulletin services], October 7, 2000.
99. State Council, Article 20, *Hulianwang xinxi fuwu guanli banfa* [Measures for managing Internet information services], September 25, 2000.
100. OpenNet Initiative Blog, "China Incentivizes Self-Censorship in Regulation of Online Video," January 4, 2008, <http://opennet.net/blog/2008/01/china-incentivizes-self-censorship-regulation-online-video>.
101. State Administration of Radio, Film, and Television (SARFT) and the Ministry of Information Industry of the People's Republic of China, Article 9, Provisions on the Management of Internet Audio and Video Programming Services, December 20, 2007. Unofficial translation available at OpenNet Initiative, <http://opennet.net/news/china-provisions>.
102. Ministry of Information Industry and the State Council Information Office, *hulianwang xinwen xinxi fuwu guanli guiding* [Provisions on the administration of news information services], September 25, 2005, <http://www.isc.org.cn/20020417/ca315779.htm>; Congressional Executive Commission on China Virtual Academy, "Provisions on the Administration of Internet News Information Services."
103. State Administration of Radio, Film and Television (SARFT), *Guangdian zongju guanyu jiaqiang hulianwang shiting jiemu neirong guanli de tongzhi* [Notice for strengthening the administration of Internet audio and video programming content], March 30, 2009, <http://www.sarft.gov.cn/articles/2009/03/30/20090330171107690049.html>; Danwei, "New Rules Imposed on Internet Video Content," April 1, 2009, http://www.danwei.org/media_regulation/new_rules_imposed_on_internet.php.

104. State Administration of Radio, Film and Television (SARFT), *Guangdian zongju guanyu jiaqiang hulianwang shiting jiemu neirong guanli de tongzhi*, Section 2 (1–21).
105. *Ibid.*, Section 3.
106. State Administration of Radio, Film, and Television (SARFT) and the Ministry of Information Industry of the People's Republic of China, Article 23, Provisions on the Management of Internet Audio and Video Programming Services.
107. Paul Budde Communication Pty., Ltd., "China—New Internet Economy," April 24, 2009.
108. Interactive Investor, "China Orders 8 More Online Video-Sharing Web Sites to Shut Down," May 21, 2008, <http://www.iii.co.uk/news/?type=afxnews&articleid=6721662&action=article>.
109. Jonathan Richards, "'Chinese YouTube' Shut Down amid Censor Fears," *Times Online*, June 20, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/article4179103.ece; Loretta Chao, "Closure of Chinese Online-Video Site Sparks Concern," *Wall Street Journal*, June 20, 2008, http://online.wsj.com/article/SB121390202591089267.html?mod=2_1567_leftbox; Reuters, "Vobile Announces Commercial Deployment with Leading Video Sharing Website 56.com," March 23, 2009, <http://www.reuters.com/article/pressRelease/idUS95209+23-Mar-2009+PRN20090323>.
110. Steven Schwankert, "China Approves Video Site Youku's License," July 10, 2008, *PCWorld*, <http://pcworld.about.com/od/interne1/China-Approves-Video-Site-Youk.htm>.
111. China Internet Network Information Center, "Twenty-third Statistical Survey Report on the Internet Development in China."
112. Stephanie Wang and Robert Faris, "Welcome to the Machine," *Index on Censorship*, 37, No. 2, (May 2008): 106–113.
113. Roland Soong, "The Weng'an Mass Incident," EastSouthWestNorth blog, July 1, 2008, http://www.zonaeuropa.com/20080701_1.htm.
114. Bob Chen, "China: Let's Do Push-up!," Global Voices Online, July 7, 2008, <http://globalvoicesonline.org/2008/07/07/china-lets-do-push-up/>.
115. Roland Soong, "The Weng'an Mass Incident," EastSouthWestNorth blog, July 1, 2008, http://www.zonaeuropa.com/20080701_1.htm.
116. Xinhua News Agency, "Police Station Assaulted, Torched by Local People in Southwest China County," June 20, 2009, http://news.xinhuanet.com/english/2008-06/29/content_8456602.htm.
117. OpenNet Initiative Blog, "China's Net Nannies in Full Force after Riot in Southern China," July 2, 2008, <http://opennet.net/blog/2008/07/china%E2%80%99s-net-nannies-full-force-after-riot-southern-china>.
118. Jonathan Ansfield, "Guizhou Riots: How Much Steam Can the Machine Filter?" Newsweek blog, July 2, 2008, <http://blog.newsweek.com/blogs/beijing/archive/2008/07/02/can-the>

-propaganda-machine-filter-the-steam.aspx; OpenNet Initiative Blog, "China's Net Nannies in Full Force After Riot in Southern China," July 2, 2008, <http://opennet.net/blog/2008/07/china%E2%80%99s-net-nannies-full-force-after-riot-southern-china>.

119. OpenNet Initiative Blog, "China's Net Nannies in Full Force after Riot in Southern China," July 2, 2008, <http://opennet.net/blog/2008/07/china%E2%80%99s-net-nannies-full-force-after-riot-southern-china>.

120. Roland Soong, "The Weng'an Mass Incident," EastSouthWestNorth blog, July 1, 2008, http://www.zonaeuropa.com/20080701_1.htm.

121. Xinhua News Agency, "Final Autopsy Shows Girl in Southwest China Protest Drowned," July 10, 2008, http://news.xinhuanet.com/english/2008-07/10/content_8519852.htm.

122. Rebecca MacKinnon, "China's Censorship 2.0: How Companies Censor Bloggers," *First Monday*, 14, No. 2 (2009), <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2378/2089>.

123. Nart Villeneuve, "Search Monitor Project: Toward a Measure of Transparency" (Working paper, Citizen Lab, University of Toronto, June 2008), <http://www.citizenlab.org/papers/searchmonitor.pdf>.

124. Ibid.

125. China Digital Times, "Baidu's Internal Monitoring and Censorship Document Leaked (1) (Updated)," April 30, 2009, <http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked/>.

126. Xiao Qiang, "Baidu's Internal Monitoring And Censorship Document Leaked (2)," *China Digital Times*, April 29, 2009, <http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked-2/>.

127. Xiao Qiang, "Chinese Censors Cut Off Twitter, Hotmail and Flickr," *China Digital Times*, June 2, 2009, <http://chinadigitaltimes.net/2009/06/chinese-censors-cut-off-twitter-hotmail-and-flickr/>.

128. isaacmao.com, "Great Firewall vs. Social Media," March 3, 2009, <http://www.isaacmao.com/meta/2009/03/great-firewall-vs-social-media.html>.

129. Consulate-General of the People's Republic of China in Chicago, "Foreign Ministry Spokesperson Liu Jianchao's Regular Press Conference on December 16, 2008," December 17, 2008, <http://www.chinaconsulatechicago.org/eng/fyrth/t526582.htm>.

130. See China Internet Illegal Information Reporting Center, <http://ciirc.china.cn/>.

131. Xinhua News Agency, "qi bumen kaizhan zhengzhi hulianwang disu zhifeng xingdong" [Seven departments launch operation for fixing the spread of vulgarity on the internet], January 5, 2009, http://www.gov.cn/jrzg/2009-01/05/content_1196447.htm.

132. Article 41, Constitution of the People's Republic of China, <http://english.peopledaily.com.cn/constitution/constitution.html>.

133. See Paulina Hartono, "China's Emerging Land Rights Movement," December 22, 2007, *China Digital Times*, <http://chinadigitaltimes.net/2007/12/chinas-emerging-land-rights-movement/>.
134. Joshua Rosenzweig, "China's Battle over the Right to Criticize," *Far Eastern Economic Review*, May 1, 2009, <http://www.feer.com/essays/2009/may/chinas-battle-over-the-right-to-criticize>.
135. Cai Ke, "Wrongly Jailed Blogger Fights for Justice," *China Daily*, May 20, 2009, http://www.chinadaily.com.cn/china/2009-05/20/content_7793902.htm.
136. Siweiluozi's Blog, "Update: Review Underway in Wu Baoquan's Case," April 22, 2009, <http://siweiluozi.blogspot.com/2009/04/update-review-underway-in-wu-baoquans.html>; Siweiluozi's Blog, "Updated Update: Ordos Law Enforcement Officials 'Clearing Their Thoughts' Regarding Wu Baoquan," April 27, 2009, <http://siweiluozi.blogspot.com/search/label/Wang%20Shuai>.
137. Joshua Rosenzweig, "China's Battle over the Right to Criticize," *Far Eastern Economic Review*, May 1, 2009, <http://www.feer.com/essays/2009/may/chinas-battle-over-the-right-to-criticize>.
138. Ibid.
139. Jane Chen, "Officials Punished over Land Scandal," *Shanghai Daily*, April 29, 2009, http://www.shanghaidaily.com/sp/article/2009/200904/20090429/article_399326.htm.
140. Chen Wangying, "The First 'Human Flesh Search' Trial," EastSouthWestNorth blog, August 2, 2008, http://www.zonaeuropa.com/20080802_1.htm.
141. Ibid.
142. Reuters, "Man Wins Case vs 'Human Flesh Search Engine,'" December 19, 2008, <http://www.reuters.com/article/technologyNews/idUSTRE4BI1I620081219>.
143. *Wall Street Journal*: China Journal blog, "A Verdict in the Case of the 'Human Flesh Search Engine,'" December 19, 2008, <http://blogs.wsj.com/chinajournal/2008/12/19/a-verdict-in-the-case-of-the-human-flesh-search-engine/>.
144. Caijing.com, "Webmasters Found Guilty of Online Harassment," December 22, 2008, <http://english.caijing.com.cn/2008-12-22/110041383.html>.
145. Chinese Law Prof Blog, "Court Decision in 'Human Flesh Search Engine' Case" January 13, 2009, http://lawprofessors.typepad.com/china_law_prof_blog/2009/01/court-decision.html.
146. Xinhua News Agency, "Law Amendments Adopted to Protect Personal Information, Punish Bribe-Taking Relatives of Officials," February 28, 2009, http://news.xinhuanet.com/english/2009-02/28/content_10916168.htm; Li Xinran, "Xuzhou Shuts Down 'Human Flesh Search Engine,'" *Shanghai Daily*, January 20, 2009, http://www.shanghaidaily.com/sp/article/2009/200901/20090120/article_388687.htm.
147. Rebecca Ruiz, "Who Will Be Watching You in Beijing?" *Forbes.com*, July 8, 2008, http://www.forbes.com/travel/2008/07/08/olympics-security-privacy-forbeslife-olympics08-cx_rr_0708security.html.

148. Ministry of Public Security, *Guojia fazhigaiwei zhuchi zhaokai dahui tongguo "jindun gongcheng" jianshe xiangmu guojia yanshou* [National development and reform commission issues national approval for the "Golden Shield" construction project at management conference], November 17, 2006, <http://www.mps.gov.cn/cenweb/brj/Cenweb/jsp/common/article.jsp?inford=ABC00000000000035645> (accessed May 25, 2009); Greg Walton, "China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China," International Center for Human Rights and Democratic Development, October 2001, <http://www.dd-rd.ca/site/publications/index.php?id=1266&subsection=catalogue>.

149. *China Tech News*, "Safe-City Project Home for New Chinese IP Video Surveillance Technology," March 11, 2008, <http://www.chinatechnews.com/2008/03/11/6475-safe-city-project-home-for-new-chinese-ip-video-surveillance-technology/>; Reuters, "China Security and Surveillance Announces Additional Safe City Project Win in Yinchuan," July 30, 2008, <http://www.reuters.com/article/pressRelease/idUS125704+30-Jun-2008+PRN20080630>.

150. Kathrin Hille, "China Bolsters Internet Censors' Scrutiny," *Financial Times*, January 5, 2009, http://www.ft.com/cms/s/0/f858f9aa-dac8-11dd-8c28-000077b07658,dwp_uuid=9c33700c-4c86-11da-89df-0000779e2340.html.

151. TRS Information Technology, "About TRS," 2008, <http://www.trs.com.cn/en/TRS/about/>.

152. *Ibid.*

153. Ministry of Information Industry, Article 3, *Huliangwang dianzi youjian fuwu guanli banfa* [Measures for the management of e-mail services], November 7, 2005.

154. Chinese cyber dissidents and activists, such as the journalist Shi Tao, have been convicted in part because of some e-mail service providers' disclosure of their users' personal information to the Chinese police. See Reporters Without Borders, "Cyber-Dissident Convicted on Yahoo! Information Is Freed after Four Years," November 9, 2006, http://www.rsf.org/article.php3?id_article=8453; Human Rights in China, "Case Highlight, Shi Tao and Yahoo," 2005, <http://hrchina.org/public/highlight/index.html>.

155. Dui Hua News blog, "Police Document Sheds Additional Light on Shi Tao Case," July 25, 2007, <http://www.duihua.org/2007/07/police-document-sheds-additional-light.html>.

156. Human Rights Watch, "Freedom of Expression and the Internet in China," August 1, 2001, <http://www.hrw.org/background/asia/china-bck-0701.htm>; Alfred Hermida, "Behind China's Internet Red Firewall," BBC News, September 3, 2002, <http://news.bbc.co.uk/1/low/technology/2234154.stm>.

157. Phillip Pan, "Chinese Crack Down on Student Web Sites," *Washington Post*, March 24, 2005, <http://www.washingtonpost.com/wp-dyn/articles/A61334-2005Mar23.html>.

158. Xinhua News Agency, "Internet Real-Name Registration System: Why So Difficult to Implement? An Investigation into the Implementation of the Hangzhou Regulations for Network Security Protection," May 19, 2009, http://news.xinhuanet.com/newscenter/2009-05/19/content_11399392.htm; David Bandurski, "Xinhua: Hangzhou's 'Real-Name Web Registration System' Is 'on the Shelf,'" China Media Project, May 20, 2009, <http://cmp.hku.hk/2009/05/20/1632/>.

159. *China Digital Times*, "Beijing Mobile's Plan for Real Name Registration of Easyown Cell Phone Numbers," January 24, 2008, <http://chinadigitaltimes.net/2008/01/beijing-mobiles-plan-for-real-name-registration-for-easyown-cell-phone-numbers/>.
160. State Council, Article 14, *Hulianwang xinxi fuwu guanli banfa* [Measures for managing Internet information services], September 25, 2000.
161. China Internet Network Information Center, "Statistical Survey Report on the Internet Development in China," March 23, 2009, <http://www.cnnic.net.cn/uploadfiles/pdf/2009/3/23/131303.pdf>.
162. State Council, Articles 19, 21, 23, *Hulianwang shangwang fuwu guanye changsuo guanli tiaolie* [Regulations on the administration of business sites providing Internet services], September 29, 2002.
163. Ministry of Information Industry, Article 14, *Hulianwang dianzi gonggao fuwu guanli guiding* [Rules on the management of Internet electronic bulletin services], October 7, 2000.
164. Chinese Human Rights Defenders, "*zhengfu ruhe jiankong women de dianzi wangluo tongxu*" [How does government monitor our online communication?], http://crd-net.org/Article/Class1/200803/20080324093843_8168.html.
165. Ibid.
166. Nart Villeneuve, "Breaching Trust: An Analysis of Surveillance and Security Practices on China's TOM-Skype Platform," Information Warfare Monitor/ONI Asia, October 1, 2008, <http://www.nartv.org/mirror/breachingtrust.pdf>.
167. John Markoff, "Surveillance of Skype Messages Found in China," *New York Times*, October 1, 2008, <http://www.nytimes.com/2008/10/02/technology/internet/02skype.html?pagewanted=all>.
168. Sky Canaves, "Skype Responds to China Surveillance Report," *Wall Street Journal Blogs: China Journal*, October 2, 2008, http://blogs.wsj.com/chinajournal/2008/10/02/skype-response-on-china-surveillance-report/?mod=googlenews_wsj.
169. Sumner Lemon, "China Tightens Surveillance of Internet Forums," *The Standard*, March, 2005, <http://archive.thestandard.com/internetnews/002807.php>.
170. Reporters Without Borders, "'Living Dangerously on the Net,'" May 12, 2003, http://www.rsf.org/article.php3?id_article=6793.
171. Phillip Pan, "Chinese Crack Down on Student Web Sites," *Washington Post*, March 24, 2005, <http://www.washingtonpost.com/wp-dyn/articles/A61334-2005Mar23.html>.
172. Australia Broadcasting Corporation, "China's Mobile Network: A Big Brother Surveillance Tool?" January 28, 2008, <http://www.abc.net.au/news/stories/2008/01/28/2147712.htm>.
173. *China Business Daily*, "*tongxin duanxiaoxi fuwu guanli guiding jijiang chutai*" [Regulation on the management of short message service will soon come into being], March 27, 2008, <http://www.txxx.com/news/article.php?id=7544>; Australia Broadcasting Corporation, "China's Mobile

Network.”; Chinese Human Rights Defenders, “*zhengfu ruhe jiankong women de dianzi wangluo tongxu*” [How does government monitor our online communication?], http://crd-net.org/Article/Class1/200803/20080324093843_8168.html.

174. Australia Broadcasting Corporation, “China’s Mobile Network: A Big Brother Surveillance Tool?” January 28, 2008, <http://www.abc.net.au/news/stories/2008/01/28/2147712.htm>.

175. Ibid.

176. Brian Krebs, “Cyber Attacks Target Pro-Tibet Groups,” *Washington Post*, March 21, 2008, <http://www.washingtonpost.com/wp-dyn/content/article/2008/03/21/AR2008032102605.html>.

177. Information Warfare Monitor, “Tracking GhostNet: Investigating a Cyber Espionage Network” (Citizen Lab/the SecDev Group), March 29, 2009, <http://www.tracking-ghost.net>.

178. Human Rights Watch, “In the Words of Chinese Officials,” June 13, 2008, http://china.hrw.org/in_the_words_of_chinese_officials.

179. Xinhua News Agency, “Openness to Foreign Media to Remain after Games,” July 30, 2008, http://www.chinadaily.com.cn/china/2008-07/30/content_6890786.htm.

180. Jacquelin Magnay, “Fury Vented at Great Firewall of China,” *Sydney Morning Herald*, July 28, 2008, <http://www.smh.com.au/news/beijing2008/reporters-vent-fury-at-great-firewall-of-china/2008/07/27/1217097058479.html>.

181. Katie Thomas, “Officials Investigate Reports of Censorship at Olympic Press Center,” *New York Times*, Jul 29, 2008, <http://olympics.blogs.nytimes.com/2008/07/29/officials-investigate-reports-of-censorship-at-olympic-press-center/?hp>.

182. Nick Mulvenney, “Update 1—Olympics—IOC Admits to Deal with China on Censorship,” Reuters, July 30, 2008, <http://www.reuters.com/article/olympicsNews/idUSPEK15086520080730?sp=true>.

183. Xinhua News Agency, “Beijing Olympic Press Centers Open,” July 8, 2008, http://news.xinhuanet.com/english/2008-07/08/content_8509880.htm

184. Keith Bradsher, “China Blocks Access to the Times’s Web Site,” *New York Times*, December 19, 2008, <http://www.nytimes.com/2008/12/20/world/asia/20china.html>.

185. Miguel Helft, “YouTube Blocked in China, Google Says,” *New York Times*, March 24, 2009, http://www.nytimes.com/2009/03/25/technology/internet/25youtube.html?_r=1&hp.

186. See Herdict Web Site Report, “www.blogger.com in China,” as of May 25, 2009, <http://www.herdic.org/web/explore/detail/id/CN/2488>.

187. Tania Branigan, “China Blocks Twitter, Flickr and Hotmail Ahead of Tiananmen Anniversary,” *Guardian*, June 2, 2009, <http://www.guardian.co.uk/technology/2009/jun/02/twitter-china>.

188. See Rebecca MacKinnon, “Original Government Document Ordering ‘Green Dam’ Software Installation,” RConversation Blog, June 8, 2009, <http://rconversation.blogs.com/rconversation/2009/06/original-government-document-ordering-green-dam-software-installation.html>.

189. Ministry of Industry and Information Technology, *guanyu jisuanji yuzhuang luse shangwang guolu ranjian de tongzhi* [Notice regarding the pre-installation of “green” online filtering software on computers], May 19, 2009, <http://tech.sina.com.cn/it/2009-06-09/17073163327.shtml>; Human Rights in China, “Chinese Government Orders Computer Manufacturers to Pre-install Filtering Software,” June 8, 2009, http://www.hrichina.org/public/contents/press?revision_id=169834&item_id=169820; Xinhua News Agency, “Anti-porn Filter Software Stirs Up Disputes in China,” June 11, 2009, http://news.xinhuanet.com/english/2009-06/11/content_11522822.htm.

190. Ministry of Industry and Information Technology, *guanyu jisuanji yuzhuang luse shangwang guolu ranjian de tongzhi* [Notice regarding the pre-installation of “green” online filtering software on computers], May 19, 2009, <http://tech.sina.com.cn/it/2009-06-09/17073163327.shtml>.

191. OpenNet Initiative, “China’s Green Dam: The Implications of Government Control Encroaching on the Home PC,” June 12, 2009, <http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc>.

192. Ibid.

193. Ibid.

194. Ibid.

195. Scott Wolchok, Randy Yao, and J. Alex Halderman, “Analysis of the Green Dam Censorware System,” Computer Science and Engineering Division, University of Michigan, June 11, 2009, <http://www.cse.umich.edu/~jhalderm/pub/gd/>.

196. OpenNet Initiative, “China’s Green Dam: The Implications of Government Control Encroaching on the Home PC,” June 12, 2009, <http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc>.

